(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－143780

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ
	12/00	５３７		12/00	５３７Ｈ
	17/30		Ｇ０９Ｃ	1/00	６３０Ａ
Ｇ０９Ｃ	1/00	６３０			６６０Ｄ
		６６０	Ｇ０６Ｆ	15/40	３２０Ａ

審査請求　未請求　請求項の数10　ＦＤ　（全 22 頁）

(21)出願番号　特願平9－319010

(22)出願日　平成９年(1997)11月５日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　茶谷　誠一
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報・通信開発本部内

(72)発明者　北川　譲
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報・通信開発本部内

(72)発明者　松永　和男
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

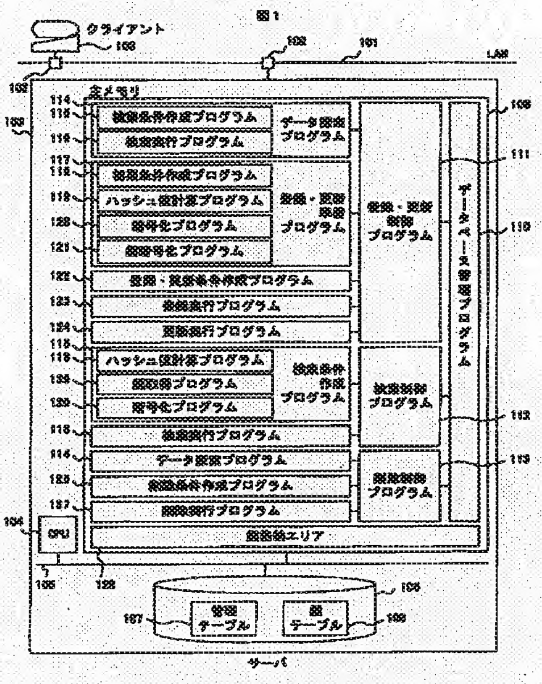
(74)代理人　弁理士　笹岡　茂　（外１名）

(54)【発明の名称】　データベースにおける秘密情報管理方法およびデータベースの秘密情報管理装置

(57)【要約】

【課題】　暗号化に関する情報を専用のテーブルを使って管理することにより、暗号化するデータベースの柔軟性と安全性を向上する。

【解決手段】　暗号化するデータベースの管理テーブル１０７とそのテーブルに対応する鍵テーブル１０８により、暗号化データを管理する。鍵テーブル１０８は特定の値の集合（１つの行の中の１つの列の項目、行、列）ごとに暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値を持つ。管理テーブル１０７へのデータの登録または更新ごとにデータ暗号化プログラム１１２において暗号鍵を作成し、さらに該暗号鍵を鍵暗号鍵を用いて暗号化し、これを鍵テーブル１０８に登録する。暗号データの検索は、ハッシュ値によって得られる暗号鍵を鍵暗号鍵を用いて復号し、復号した暗号鍵と暗号化アルゴリズムを用いて行う。これによりデータベース稼動中に暗号鍵や暗号化アルゴリズムの変更を可能にする。



1

【特許請求の範囲】

【請求項１】　暗号化された秘密情報を管理するデータベースにおける秘密情報管理方法であって、

前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを設け、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、

前記データベースへの秘密情報の登録時に、

シリアル番号を作成し、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録し、

前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化し、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算し、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録することを特徴とするデータベースにおける秘密情報管理方法。

【請求項２】　請求項１記載の秘密情報管理方法において、

前記データベースに登録された秘密情報の検索時に、

検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出し、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出し、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号し、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行うことを特徴とするデータベースにおける秘密情報管理方法。

【請求項３】　請求項２記載のデータベースにおける秘密情報管理方法において、

検索条件に一致する秘密情報を検索後に、

該検索した秘密情報を暗号化するための新たな鍵を乱数を使って作成し、該作成した鍵により該検索した秘密情報を暗号アルゴリズムを用いて新たに暗号化し、該作成した鍵を前記鍵暗号鍵により暗号化し、該新たに暗号化した秘密情報で管理テーブルを更新し、前記鍵暗号鍵により暗号化した暗号化のための新たな鍵と前記暗号アルゴリズムの識別子により鍵テーブルを更新することを特徴とするデータベースにおける秘密情報管理方法。

2

【請求項４】　請求項２記載のデータベースにおける秘密情報管理方法において、

前記データベースに登録された秘密情報の更新時に、

更新前の秘密情報と更新後の秘密情報を入力し、更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得し、

前記更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録し、

前記作成した鍵を前記鍵暗号鍵により暗号化し、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録することを特徴とするデータベースにおける秘密情報管理方法。

【請求項５】　暗号化された秘密情報を管理するデータベースの秘密情報管理装置であって、

前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、

秘密情報の登録時にシリアル番号を作成する手段と、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録する手段と、

前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手段と、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算する手段と、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録する手段と、

秘密情報の検索時に検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出す手段と、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出す手段と、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号する

手段と、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行う手段を備えることを特徴とするデータベースの秘密情報管理装置。

【請求項６】　請求項５記載のデータベースの秘密情報管理装置において、

秘密情報の更新時に、入力された更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得する手段と、入力された更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録する手段と、

前記作成した鍵を前記鍵暗号鍵により暗号化する手段と、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録する手段を備えることを特徴とするデータベースにおけるデータベースの秘密情報管理装置。

【請求項７】　暗号化された秘密情報と暗号化に用いた鍵情報を記録したコンピュータ読み取り可能な記録媒体であって、

前記暗号化された秘密情報は管理テーブルに記録され、

前記暗号化に用いた鍵情報は鍵テーブルに記録され、

前記管理テーブルは、複数の行と複数の列からなり、各行対応に暗号化された秘密情報の組が記録され、

前記鍵テーブルは、複数の行と複数の列からなり、前記管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値が記録され、

前記管理テーブルと鍵テーブルの各行には管理テーブルの行と鍵テーブルの行を互いに関連付けるシリアル番号が記録されたことを特徴とする暗号化された秘密情報と暗号化に用いた鍵情報を記録したコンピュータ読み取り可能な記録媒体。

【請求項８】　暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースへの秘密情報の登録時にシリアル番号を作成する手順と、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化する手順と、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録する手順と、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手順と、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算する手順と、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録する手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項９】　暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースへの秘密情報の検索時に検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出す手順と、該条件一致行から、秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出す手順と、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号する手順と、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行う手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースに登録された秘密情報の更新時に、入力された更新前の秘密情報によりデータベースを検索

し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得する手順と、入力された更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化する手順と、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録する手順と、前記作成した鍵を秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手順と、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録する手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、秘密情報をデータベースに暗号化して登録し、管理する方法に関するものである。

【０００２】

【従来の技術】昨今、データベースは、クレジット会社、銀行など様々な分野で利用されている。特に最近では、電子商取引の認証を行う認証局も、認証のために氏名やクレジット番号などの個人の秘密情報を管理するデータベースを持っている。このようなデータベースは個人に関する秘密情報を扱っているため、例えばデータベースを操作できるアクセス権をデータベース管理者のような特定の個人にしか与えないようにすることにより、データの漏洩を防いでいる。しかしながら、データベースへのアクセス権を設定している場合でも、不正な侵入者がデータベースを記録した記憶装置を不正に持ち出し、該装置の内容を直接見ることによりデータが漏洩する危険性がある。そこで、氏名やクレジット番号など特定の情報を暗号化して登録し、情報を取り出すときに復号して元の情報を得ることによりセキュリティを確保することが考えられる。このように特定の情報を暗号化しておくことにより、データベースが記録された装置が盗難にあったとしても復号のための鍵が盗まれていなければ、情報が漏洩する危険性は大幅に減少する。従来は、このような情報の暗号化に特定の一つの鍵を用いて、データベース全体を暗号化していた。

【０００３】データベースを暗号化する技術の例としては「特開平８－３２９０１１」に開示されているものがある。該公知例の実施例は、データベース、鍵管理センタ、１次ユーザ、２次ユーザを相互に接続するネットワークシステムから構成される。１次ユーザは著作権情報を暗号化してデータベースに格納し、鍵を鍵管理センタに格納する。２次ユーザがその著作権情報を利用するときは、鍵管理センタから暗号鍵をもらい、そのときに課金される方式が提案されている。この公知例の鍵管理センタは、保管されている鍵と著作権ラベルの対応づけを

行うことによって鍵を管理している。

【０００４】

【発明が解決しようとする課題】従来の技術では、特定の一つの暗号鍵でデータベース全体を暗号化したデータベースでは、その暗号鍵がデータベースが記録された装置と同時に盗難にあった場合、データベース全体が解読され、秘密情報が漏洩する危険性がある。また、データベースの稼動中に暗号鍵が盗難にあった場合、不正侵入者がこの鍵を使用してデータを解読する可能性がある。従って、これらの状況においては暗号鍵を変更してデータの漏洩を防止する必要が生じる。暗号鍵を変更するためには、データベースに対するユーザからのアクセスを禁止し、データベース中のすべてのデータを一旦復号化した後で新しい暗号鍵で暗号化し直さなければならない。データベースの規模が大きくなればなるほどこの作業には時間がかかり、その間、ユーザはデータベースにアクセスできない。さらに鍵が盗難に会わなくとも、暗号化されたデータのうち一つが解読されると、データベースを暗号化している鍵が一つであるため、他のデータがすべて解読される危険性がある。

【０００５】また、従来の技術ではデータベースの稼動中に、より強固な暗号化アルゴリズムを採用してセキュリティを高めようとする場合に、暗号化アルゴリズムを変更することが困難である。なぜなら、この場合にもデータベースへのユーザアクセスを一旦禁止し、すべてのデータを新しい暗号化アルゴリズムで暗号化し直さなければならないからである。以上で述べたように、従来のデータベースを暗号化する方式においては、データベースを暗号化する鍵が１つであるためその鍵が盗難に合った場合、その鍵で暗号化されたデータベースがすべて解読され秘密情報が漏洩する危険性があり、また暗号化したデータベース稼働中により強固な暗号化アルゴリズムが発明されたとしてもデータベースの暗号化アルゴリズムをその方式に変更するのは困難であるという問題があった。

【０００６】本発明は、データベースを暗号化する方式において、データベースの内容を漏洩しない安全なデータベースの秘密情報管理方式を提供すること、暗号鍵や暗号化アルゴリズムの変更をデータベース稼働中にも容易に行うことができるようにすること、および複数の暗号化アルゴリズムと複数の暗号鍵を使うことができるようにすることを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号化された秘密情報を管理するデータベースにおける秘密情報管理方法であって、前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム

識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを設け、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、前記データベースへの秘密情報の登録時に、シリアル番号を作成し、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録し、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化し、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算し、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録するようにしている。

【０００８】また、前記データベースに登録された秘密情報の検索時に、検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出し、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出し、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号し、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行うようにしている。

【０００９】また、検索条件に一致する秘密情報を検索後に、該検索した秘密情報を暗号化するための新たな鍵を乱数を使って作成し、該作成した鍵により該検索した秘密情報を暗号アルゴリズムを用いて新たに暗号化し、該作成した鍵を前記鍵暗号鍵により暗号化し、該新たに暗号化した秘密情報で管理テーブルを更新し、前記鍵暗号鍵により暗号化した暗号化のための新たな鍵と前記暗号アルゴリズムの識別子により鍵テーブルを更新するようにしている。

【００１０】また、前記データベースに登録された秘密情報の更新時に、更新前の秘密情報と更新後の秘密情報を入力し、更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得し、前記更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録し、前記作成した鍵を前記鍵暗号鍵により暗号化し、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録するようにしている。

【００１１】

【発明の実施の形態】まず、本発明の原理について説明する。秘密情報を管理するデータベースは、暗号化された秘密情報を格納するための管理テーブルと、その管理テーブルの１つの行の中の１つの列の項目（以下では、フィールドと称する）、行、または列などの特定の値の集合ごとに該集合に属する個々の値を暗号化するために使用した鍵と暗号アルゴリズム識別子を格納する鍵テーブルを有する。前記管理テーブルと鍵テーブルは、２つのテーブルの行を関連付けるシリアル番号をそれぞれ格納しており、前記管理テーブルの特定の値の集合を結合した値に対して計算したハッシュ値も鍵テーブルに格納する。暗号化した秘密情報の登録には、まず、秘密情報を暗号化するための鍵（以下では、データ暗号鍵と称する）を乱数を使って作成する。そのデータ暗号鍵を使って管理テーブルに登録する秘密情報を暗号化する。このような鍵の例としてＭＵＬＴＩ２、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等がある。さらに、前記データ暗号鍵は、秘密情報を暗号化する鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する別の鍵（以下では、鍵暗号鍵と称する）を用いて暗号化される。そして、秘密情報の検索のために使用するハッシュ値を暗号化前の秘密情報から計算する。さらに、シリアル番号を生成し、シリアル番号と暗号化された秘密情報を管理テーブルに登録し、シリアル番号とデータ暗号鍵と暗号化アルゴリズム識別子とハッシュ値を鍵テーブルに登録する。

【００１２】検索条件としてシリアル番号が指定された場合は、鍵テーブルにおいてそのシリアル番号を検索し、鍵テーブルからそのシリアル番号に一致する暗号化アルゴリズム識別子と暗号化されたデータ暗号鍵を取り出し、鍵暗号鍵で暗号化されたデータ暗号鍵を復号する。次に管理テーブルにおいてシリアル番号を検索し、管理テーブルから、シリアル番号に一致する暗号化された秘密情報を取り出し、その秘密情報を前記暗号アルゴリズムで前記データ暗号鍵を使って復号する。検索条件として秘密情報のみが指定された場合は、まず、検索条件のハッシュ値を計算する。そのハッシュ値により鍵テーブルを検索してそのハッシュ値に一致する暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子をすべて取り出し、前記暗号化されたデータ暗号鍵を復号したデータ暗号鍵と、暗号化アルゴリズムにより検索条件を暗号化する。次に、暗号化した検索条件を使って管理テーブルを検索し、一致する秘密情報を含む行が見つかった場合、その行のシリアル番号に対応する鍵テーブルの他の暗号化されたデータ暗号鍵を復号した鍵と暗号化アルゴリズム識別子を使って、検索条件以外の秘密情報を復号する。

【００１３】以上説明した原理を、さらに具体例を用いて説明する。本例で用いる管理テーブルの例を図２に示し、その管理テーブルに対応する鍵テーブルを図３に示す。管理テーブルの列は、シリアル番号、名前、電話番号、住所で構成され、鍵テーブルの列は、シリアル番号、名前のハッシュ値、名前暗号アルゴリズム識別子、名前の暗号鍵、電話番号のハッシュ値、電話番号暗号アルゴリズム識別子、電話番号の暗号鍵、住所のハッシュ値、住所暗号アルゴリズム識別子、住所の暗号鍵で構成される。図２、図３において、天地逆の文字は暗号化されているデータを示している。図２の管理テーブルには、名前、電話番号が暗号化され、住所が暗号化されないで格納されている。図３の鍵テーブルには、名前、電話番号、住所のそれぞれのハッシュ値、暗号化アルゴリズム識別子、暗号鍵が格納され、このうち暗号鍵は暗号化されて格納されている。

【００１４】本例で、シリアル番号の項目２００の列が「１１」の行２０４と、シリアル番号の項目２００の列が「１２」の行２０５が、管理テーブルに格納されており、シリアル番号の項目３００の列が「１１」の行３１０と、シリアル番号の項目３００の列が「１２」の行３１１が、鍵テーブル１０８に格納されている状態で、新たに名前「日立花子」、電話番号「９８７－６５４３」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「９８７－６５４３」を暗号化するための鍵を乱数を使ってそれぞれ作成し、「３１５ＴＫ８」「１２３ＡＢＤ」を求める。次に作成した鍵「３１５ＴＫ８」を使って「日立花子」を暗号化プログラムが持つ最新の暗号アルゴリズムで暗号化し、鍵「１２３ＡＢＤ」を使って「９８７－６５４３」を前記暗号アルゴリズムで暗号化する。次に「日立花子」からハッシュ値「５０２」を計算し、「９８７－６５４３」からハッシュ値「１４３」を計算し、「東京都」からハッシュ値「１２３」を計算する。鍵「３１５ＴＫ８」、「１２３ＡＢＤ」を鍵暗号鍵で暗号化する。管理テーブルと鍵テーブルの行を関係付けるシリアル番号「１３」を生成し、管理テーブルのシリアル番号の項目２０７に「１３」、名前の項目２０８に暗号化された「日立花子」、電話番号の項目２０９に暗号化された「９８７－６５４３」、住所の項目２１０に「東京都」を登録し、鍵テーブルのシリアル番号の項目３１２に「１３」、名前のハッシュ値の項目３１３に「５０２」、名前の暗号化アルゴリズム識別子の項目３１４に「２」、名前の暗号鍵の項目３１５に暗号化された「３１５ＴＫ８」、電話番号のハッシュ値の項目３１６に「１４３」、電話番号の暗号化アルゴリズム識別子の項目３１７に「２」、電話番号の暗号鍵の項目３１８に暗号化された「１２３ＡＢＤ」、住所のハッシュ値の項目３１９に「１２３」、住所の暗号化アルゴリズム識別子の項目３２０に「０」を登録する。

【００１５】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」の電話番号を検索する場合について説明する。まず、「日立二郎」からハッシュ値を計算し、ハッシュ値「３５９」を求める。鍵テーブルの名前のハッシュ値で「３５９」を検索して、その暗号化アルゴリズム識別子「１」３２２と暗号化されたデータ暗号鍵「ＺＸＢ５１５」３２３を取り出す。次にデータ暗号鍵を鍵暗号鍵で復号する。復号した暗号鍵「ＺＸＢ５１５」３２３と暗号化アルゴリズム識別子「１」３２２を使って名前の検索条件「日立二郎」を暗号化する。暗号化された「日立二郎」の検索条件を使って管理テーブルを検索する。管理テーブルにおいて暗号化された「日立二郎」を検索し、その行のシリアル番号「１２」２１１を取り出し、そのシリアル番号「１２」２１１を使って鍵テーブルの電話番号の暗号化アルゴリズム識別子「１」３２４と暗号化されたデータ暗号鍵「０１ＥＲ８８」を鍵暗号鍵で復号した鍵を使って管理テーブル上の「日立二郎」の暗号化された電話番号を復号化する。

【００１６】次に、各行に含まれる値のそれぞれに同一のデータ暗号鍵を使用し、かつ各行ごとに異なるデータ暗号鍵を使用する場合について説明する。この場合の管理テーブルと鍵テーブルの例を図４、図５に示す。図４は、行ごとに暗号化された管理テーブルの例である。図４のテーブル構成は図２と同じであるが、暗号化されて格納されている単位が図２と異なり、行ごとになっている。図４において、天地逆の文字は暗号化されているデータを示している。図４の管理テーブルに対応する鍵テーブルの例を図５に示す。図５の鍵テーブルは、シリアル番号、名前と電話番号を連結した値のハッシュ値、暗号化アルゴリズム識別子、およびデータ暗号鍵を列に持つ。鍵テーブルは行ごとに暗号化した鍵を持つのでハッシュ値、暗号化アルゴリズム識別子、暗号鍵は行ごとに１つだけ存在する。図５において、天地逆の文字は暗号化されているデータを示している。シリアル番号の項目の列５００は、管理テーブルと鍵テーブルの行を関連付けるためのシリアル番号を格納する。図５では、名前、電話番号の２つを組み合わせて計算されるハッシュ値を、名前、電話番号のハッシュ値の項目の列５０１に格納しているが、これは名前だけの１つからハッシュ値を計算するようにしてもよい。図４の管理テーブルと図５の鍵テーブルの構造を持つデータベースにより、行ごとにそれぞれ別のデータ暗号鍵で暗号化することが可能となる。

【００１７】本例で、シリアル番号の項目の列４００が「１１」の行４０４と、シリアル番号の項目の列４００が「１２」の行４０５が、管理テーブルに格納されており、シリアル番号の項目の列５００が「１１」の行５０４と、シリアル番号の項目の列５００が「１２」の行５０５が、鍵テーブルに格納されている状態で、新たに名

前「日立花子」、電話番号「９８７－６５４３」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「９８７－６５４３」、「東京都」を暗号化するための鍵を乱数を使って１つ作成し、「３１５ＴＫ８」を求める。次に作成した鍵「３１５ＴＫ８」を使って「日立花子」、「９８７－６５４３」、「東京都」をそれぞれ暗号化プログラムが持つ最新の暗号アルゴリズムで暗号化する。次に「日立花子」、「９８７－６５４３」からハッシュ値「５３２」を計算する。鍵「３１５ＴＫ８」を鍵暗号鍵で暗号化する。管理テーブルと鍵テーブルの行を関係付けるシリアル番号「１３」を生成し、管理テーブルのシリアル番号の項目４０７に「１３」、名前の項目４０８に暗号化された「日立花子」、電話番号の項目４０９に暗号化された「９８７－６５４３」、住所の項目４１０に暗号化された「東京都」を登録し、鍵テーブルのシリアル番号の項目５０６に「１３」、名前、電話番号のハッシュ値の項目５０７に「５３２」、暗号化アルゴリズム識別子の項目５０８に「１」、暗号鍵の項目５０９に暗号化された「３１５ＴＫ８」を登録する。

【００１８】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」で電話番号が「１２３－４５６７」の住所を検索する場合について説明する。行ごとに暗号化されたデータベースにおいて暗号化された情報を検索する場合、ハッシュ値を計算するために使用した項目はすべて検索条件の中に指定しなければならない。まず、「日立二郎」、「１２３－４５６７」からハッシュを計算し、ハッシュ値「４５９」を求める。鍵テーブルの名前、電話番号のハッシュ値で「４５９」を検索して、その暗号化アルゴリズム識別子「１」５１２と暗号化されたデータ暗号鍵「ＰＢ２４ＣＳ」５１３を取り出す。次にデータ暗号鍵を鍵暗号鍵で復号する。

【００１９】取り出した暗号鍵「ＰＢ２４ＣＳ」５１３と暗号化アルゴリズム識別子「１」５１２を使って「日立二郎」、「１２３－４５６７」を暗号化した検索条件を作成する。暗号化された「日立二郎」、「１２３－４５６７」の検索条件を使って管理テーブルを検索する。管理テーブルにおいて暗号化された「日立二郎」、「１２３－４５６７」を検索し、一致する行が管理テーブルにあれば、「日立二郎」、「１２３－４５６７」を暗号化した鍵と暗号化アルゴリズムを使って、シリアル番号が「１２」の行の管理テーブルの暗号化された住所を復号化する。

【００２０】暗号化する特定の集合が列の場合の管理テーブルと鍵テーブルの例を図６、図７に示す。図６のテーブル構成はシリアル番号の項目がない点が図２と異なる。図６において、天地逆の文字は暗号化されているデータを示している。図６では住所の項目６０２のデータは暗号化されないで格納されている。図６の管理テーブルに対応する鍵テーブルの例を図７に示す。図７において、天地逆の文字は暗号化されているデータを示している。図７は、各列に含まれる値のそれぞれに同一のデータ暗号鍵を使用し、かつ各列ごとに異なるデータ暗号鍵を使用する場合の鍵テーブルの例である。この場合は、列ごとにすべての行が同じ暗号鍵と暗号化アルゴリズムを使うので、ハッシュ値を格納しない。図６の管理テーブルと図７の鍵テーブルの構造を持つデータベースにより、列ごとにそれぞれ別の暗号鍵を持つデータベースの暗号化が可能となる。

【００２１】本例で、管理テーブルの行６０３と行６０４が、管理テーブルに格納されており、行７１１が、鍵テーブルに格納されている状態で、新たに名前「日立花子」、電話番号「９８７－６５４３」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「９８７－６５４３」を暗号化するための鍵を取得する。そのために鍵暗号鍵で暗号化された「２４Ｂ５２Ｃ」、「ＳＷ６１０Ｖ」と暗号アルゴリズム識別子「１」、「１」を鍵テーブルから取得し、鍵暗号鍵で暗号化された「２４Ｂ５２Ｃ」、「ＳＷ６１０Ｖ」を鍵暗号鍵で復号する。次に取得した鍵「２４Ｂ５２Ｃ」を使って「日立花子」を鍵テーブルから取り出した暗号アルゴリズムで暗号化し、鍵「ＳＷ６１０Ｖ」を使って「９８７－６５４３」を前記暗号化アルゴリズムで暗号化する。

【００２２】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」の電話番号を検索する場合について説明する。まず、鍵テーブルから名前の暗号化アルゴリズム識別子「１」７０６と暗号化されたデータ暗号鍵「２４Ｂ５２Ｃ」７０７を取り出す。次に暗号化されたデータ暗号鍵「２４Ｂ５２Ｃ」を鍵暗号鍵で復号する。前記データ暗号鍵「２４Ｂ５２Ｃ」７０７を暗号化アルゴリズム識別子「１」７０６を使って名前の検索条件「日立二郎」を暗号化する。暗号化された「日立二郎」の検索条件を使って管理テーブルを検索する。「日立二郎」の行の暗号化された電話番号を鍵テーブルの電話番号の暗号鍵「ＳＷ６１０Ｖ」７０９を復号化したものと暗号化アルゴリズム識別子「１」を使って復号化する。

【００２３】以上のように、秘密情報を暗号化して登録するデータベースにおいて、暗号化した秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルの２つを使って管理することにより、管理テーブルの特定の値の集合ごとに暗号鍵と暗号化アルゴリズムを変更することが可能となる。

【００２４】以下、本発明の第一の実施例について図１

を用いて説明する。本システムは、クライアント１００、ＬＡＮ１０１、ＬＡＮアダプタ１０２、サーバ１０３から構成される。クライアント１００とサーバ１０３は、ＬＡＮアダプタ１０２を介してＬＡＮ１０１により接続される。サーバ１０３は、ＣＰＵ１０４、主メモリ１０９、バス１０５、磁気ディスク装置１０６から構成される。主メモリ１０９と磁気ディスク装置１０６は、ＣＰＵ１０４よりバス１０５を介してアクセスされる。主メモリ１０９には、データベース管理プログラム１１０、登録・更新制御プログラム１１１、検索制御プログラム１１２、削除制御プログラム１１３、データ探索プログラム１１４、登録・更新準備プログラム１１７、登録・更新条件作成プログラム１２２、登録実行プログラム１２３、更新実行プログラム１２４、検索条件作成プログラム１１５、検索実行プログラム１１６、削除条件作成プログラム１２６、削除実行プログラム１２７および鍵格納エリア１２８が格納される。

【００２５】データ探索プログラム１１４は、検索条件作成プログラム１１５と検索実行プログラム１１６で構成される。登録・更新準備プログラム１１７は、初期条件作成プログラム１１８、ハッシュ値計算プログラム１１９、暗号化プログラム１２０、および鍵暗号化プログラム１２１で構成される。検索条件作成プログラムは、ハッシュ値計算プログラム１１９、鍵取得プログラム１２５、および暗号化プログラム１２０で構成される。磁気ディスク装置１０６には、管理テーブル１０７と鍵テーブル１０８が格納される。

【００２６】以下、図１の構成のシステムにおいて、データベースに暗号化して格納するデータの登録処理の概略について説明する。ユーザがクライアント１００からデータベースに登録するデータを入力する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力された登録するデータが登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、登録・更新準備プログラム１１７に登録するデータを渡す。登録・更新準備プログラム１１７は、初期条件作成プログラム１１８によりシリアル番号を作成し、ハッシュ値計算プログラム１１９により登録するデータのハッシュを計算し、暗号化プログラム１２０により登録するデータを暗号化する鍵を作成して、暗号化プログラム１２０が持っている最新の暗号化アルゴリズムにより登録するデータを暗号化し、さらにその暗号化の鍵を鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより鍵格納エリア１２８にある鍵で暗号化する。登録・更新準備プログラム１１７は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を登録実行プログラム１２３に渡す。登録実行プログラム１２３は、データベース管理プログラム１１０を使って管理テーブル１０７に、シリアル番号、暗号化された登録データを登録し、鍵テーブル１０８に、シリアル番号、登録されるデータのハッシュ値、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録する。

【００２７】次に、このような構成の本システムにおいて、暗号化してデータベースに登録したデータの検索処理の概略について説明する。ユーザがクライアント１００から検索するデータを入力する。検索制御プログラム１１２が起動され、クライアント１００から入力された検索するデータが検索制御プログラム１１２に渡される。検索制御プログラム１１２が検索条件作成プログラム１１５に検索するデータを渡す。検索条件作成プログラム１１５は、ハッシュ値計算プログラム１１９により検索するデータのハッシュ値を計算し、鍵取得プログラム１２５により鍵テーブル１０８から前記ハッシュ値に一致する行の暗号化された暗号鍵と、暗号化アルゴリズム識別子を取り出す。暗号化されたデータ暗号鍵を鍵暗号鍵で復号する。復号したデータ暗号鍵と暗号化アルゴリズム識別子で検索条件を暗号化し、検索のためのＳＱＬ文を作成する。検索条件作成プログラム１１５は、作成したＳＱＬ文を検索制御プログラム１１２に渡す。検索制御プログラム１１２は、前記ＳＱＬ文を検索実行プログラム１１６に渡す。検索実行プログラム１１６は、データベース管理プログラム１１０を使って暗号化された検索条件に一致するデータを管理テーブル１０７から検索する。データベース管理プログラム１１０は、検索結果を、検索制御プログラム１１２に渡す。検索制御プログラム１１２は、検索結果を復号してクライアント１００に復号した検索結果を返す。クライアント１００は、検索結果を画面に表示する。

【００２８】次に、このような構成の本システムにおいて、暗号化してデータベースに格納したデータの更新処理の概略について説明する。ユーザがクライアント１００から更新前のデータと更新後のデータを入力する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力された更新前データと更新後のデータが登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、更新前のデータをデータ探索プログラム１１４に渡す。データ探索プラグラム１

１４は、検索条件作成プログラム１１５により更新前のデータを暗号化し、検索実行プログラム１１６により更新前のデータのシリアル番号を取り出し、登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータを登録・更新準備プログラム１１７に渡す。登録・更新準備プログラム１１７は、ハッシュ値計算プログラム１１９により、更新後のデータのハッシュ値を計算し、暗号化プログラム１２０により更新後のデータを暗号化する鍵を作成し、更新するデータを暗号化プログラム１２０が持っている最新の暗号化アルゴリズムで暗号化し、さらに鍵暗号化プログラム１２１が、その暗号化の鍵を鍵格納エリア１２８にある鍵暗号鍵で鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより暗号化する。

【００２９】登録・更新準備プログラム１１７は、更新後のデータのハッシュ値、暗号化された更新後のデータ、暗号化された更新後のデータを暗号化した鍵、更新後のデータを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータのハッシュ値、暗号化された更新後のデータ、暗号化された更新後のデータを暗号化した鍵、更新後のデータを暗号化した暗号化アルゴリズム識別子を登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を更新実行プログラム１２４に渡す。更新実行プログラム１２４は、データベース管理プログラム１１０を使って、管理テーブル１０７の暗号化された更新後のデータと鍵テーブル１０８の更新後のデータのハッシュ値、暗号化された更新後のデータを暗号化した鍵、暗号化アルゴリズム識別子をシリアル番号にしたがって更新する。

【００３０】次に、このような構成の本システムにおいて、暗号化してデータベースに格納したデータの削除処理の概略について説明する。ユーザがクライアント１００から削除するデータを入力する。削除制御プログラム１１３が起動され、クライアント１００から入力された削除するデータがこれに渡される。削除制御プログラム１１３は、削除するデータをデータ探索プログラム１１４に渡す。データ探索プログラム１１４は、検索条件作成プログラム１１５により削除するデータを暗号化し、検索実行プログラム１１６により削除するデータのシリアル番号を取り出し、削除制御プログラム１１３に渡す。削除制御プログラム１１３は、前記シリアル番号を削除条件作成プログラム１２６に渡す。削除条件作成プログラム１２６は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを削除制御プログラム１１３に渡す。削除制御プログラム１１３は、削除条件作成プログラム１２６で作成したＳＱＬ文を削除実行プログラム１２７に渡す。削除実行プログラム１２７は、データベース管理プログラム１１０を使って管理テーブル１０７と鍵テーブル１０８から渡されたシリアル番号の行を削除する。

【００３１】上述の処理をフローチャートを用いて、さらに詳細に説明する。以下の説明では、具体例として図２の管理テーブルと図３の鍵テーブルを用いた場合について説明する。図８は登録・更新プログラム１１１が実行する暗号化データベースへのデータの登録処理フローを示している。

【００３２】データ登録処理は、登録データ入力ステップ８００、登録準備ステップ８０１、登録データＳＱＬ文作成ステップ８０２およびデータベース登録ステップ８０３からなる。登録データ入力ステップ８００では、ユーザがクライアント１００から入力した登録するデータを読み込む。登録準備ステップ８０１では、シリアル番号を作成し、登録するデータのハッシュ値を計算し、登録するデータを暗号化するデータ暗号鍵を作成し、そのデータ暗号鍵で登録するデータを暗号化する。データ暗号鍵を鍵暗号鍵で暗号化する。登録データＳＱＬ文作成ステップ８０２では、登録準備ステップ８０１で作成したシリアル番号、計算したハッシュ値、暗号化されたデータ暗号鍵、暗号化された登録するデータから、管理テーブル１０７と鍵テーブル１０８に登録するＳＱＬ文を作成する。データベース登録ステップ８０３では、登録実行プログラム１２３が登録データＳＱＬ文作成ステップ８０２で作成したＳＱＬ文を実行して、データベース管理プログラム１１０により管理テーブル１０７にシリアル番号と暗号化された登録するデータを登録し、鍵テーブル１０８にシリアル番号と登録データのハッシュ値と暗号化した登録データを暗号化した鍵と暗号化アルゴリズム識別子を登録する。

【００３３】次に、登録準備ステップ８０１の処理を図９のフローチャートを使って詳細に説明する。登録準備ステップ８０１は、シリアル番号作成ステップ９００、ハッシュ値計算ステップ９０１、暗号アルゴリズム決定ステップ９０２、データ暗号化ステップ９０３および鍵暗号化ステップ９０４からなる。シリアル番号作成ステップ９００では、管理テーブル１０７と鍵テーブル１０８のそれぞれの行を関係付けるシリアル番号を作成する。ハッシュ値計算ステップ９０１では、登録するデータのハッシュ値を計算する。暗号アルゴリズム決定ステップ９０２では、暗号化プログラム１２０が今回の暗号化に使用する暗号化アルゴリズムを決定する。暗号化プログラム１２０は複数の暗号アルゴリズムを持つことができ、その中で登録・更新時の暗号化にはもっとも新しく暗号化プログラム１２０に登録された暗号アルゴリズムを使用するようにしている。データ暗号化ステップ９

０３では、登録するデータを暗号化するためのデータ暗号鍵を作成し、そのデータ暗号鍵で登録するデータを暗号化する。鍵暗号化ステップ９０４では、データ暗号化ステップ９０３で作成した鍵を鍵格納エリア１２８にある鍵暗号鍵を使って暗号化する。

【００３４】図１０は検索制御プログラム１１２が実行する暗号化データベースへのデータの検索処理フローを示している。データ検索処理は、検索データ入力ステップ１０００、ハッシュ値計算ステップ１００１、検索ＳＱＬ文作成ステップ１００２、管理テーブル検索ステップ１００３、管理テーブル一致データチェックステップ１００４、鍵テーブル検索ステップ１００５、鍵テーブル一致データチェックステップ１００６、検索結果表示ステップ１００７、シリアル番号取得ステップ１００８、全データ復号ステップ１００９からなる。検索データ入力ステップ１０００では、ユーザがクライアント１００から入力した検索するデータを読み込む。ハッシュ値計算ステップ１００１では、検索するデータのハッシュ値を計算する。検索ＳＱＬ文作成ステップ１００２では、ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行の暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を鍵テーブル１０８から取り出し（ハッシュ値についてのＳＱＬ文を作成して鍵テーブルから取り出す）、データ暗号鍵を復号し、その復号したデータ暗号鍵で検索データを暗号化して、管理テーブルを検索するＳＱＬ文を作成する。管理テーブル検索ステップ１００３では、検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文により管理テーブル１０７を検索する。管理テーブル一致データチェックステップ１００４では、検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文に一致するデータが管理テーブル１０７にあるかどうか調べる。検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文に一致するデータが管理テーブル１０７にある場合、シリアル番号取得ステップ１００８に進む。シリアル番号取得ステップ１００８では、管理テーブル１０７で一致したデータの鍵テーブル１０８のシリアル番号を取り出す。全データ復号ステップ１００９では、シリアル番号取得ステップ１００８で取り出したシリアル番号からすべての暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出し、鍵暗号鍵で復号したデータ暗号鍵と、暗号化アルゴリズムにより管理テーブルの暗号化されたデータをすべて復号化する。管理テーブル検索ステップ１００３に戻り処理を続ける。

【００３５】検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文に一致するデータが管理テーブル１０７にない場合、鍵テーブル検索ステップ１００５に進み、鍵テーブル１０８を検索し、ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行がまだあるか調べる。鍵テーブル一致データチェックステップ１００６では、鍵テーブル検索ステップ１００５の検索結果を判定する。ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行がある場合、検索ＳＱＬ文作成ステップ１００２に戻り、新たなデータ暗号鍵を使って検索処理を行う。ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行がない場合、検索結果表示ステップ１００７に進む。検索結果表示ステップ１００７では、クライアントの画面に検索結果が表示される。

【００３６】次に、検索ＳＱＬ文作成ステップ１００２の処理を図１１のフローチャートを使って詳細に説明する。検索ＳＱＬ文作成ステップ１００２は、暗号化情報取得ステップ１１００および暗号化検索データ作成ステップ１１０１からなる。暗号化情報取得ステップ１１００では、鍵テーブル１０８を検索して、ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行の暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出し、暗号化されたデータ暗号鍵を鍵暗号鍵で復号する。暗号化検索データ作成ステップ１１０１では、復号したデータ暗号鍵と、暗号化アルゴリズムにより検索条件を暗号化する。

【００３７】暗号化されているデータベースを検索する方法として、暗号化された管理テーブルからデータを一つずつ取り出し、それを復号しながら検索条件に一致するかどうかを調べる方法と検索条件をあらかじめ暗号鍵で暗号化しておき、その暗号化した検索条件で暗号化された管理テーブルを検索する方法がある。前者の方法では、管理テーブルからのデータの取り出しごとに復号の処理が発生するため、データベースの検索性能を大きく悪化させる。後者の方法では、検索条件を暗号化する処理が一回発生する以外は、暗号化されていないデータベースとほぼおなじ検索性能を出すことができる。このため、暗号化された管理テーブルの検索の実現には、後者の方法が性能的に優れている。本実施例においては、後者の方式について説明した。

【００３８】本発明の方式のデータ構造では特定のデータ集合ごとに暗号化に使用する鍵が異なるため、鍵テーブル１０８から検索条件を暗号化する鍵を取り出す手段としてデータのハッシュ値を利用して鍵テーブル１０８からデータ暗号鍵を検索するようにした。

【００３９】図１２は登録・更新制御プログラム１１１が実行する暗号化データベースへのデータの更新処理フローを示している。データ更新処理は、更新データ入力ステップ１２００、更新前データ探索ステップ１２０１、一致データチェックステップ１２０２、シリアル番号取得ステップ１２０３、更新後データ暗号化ステップ１２０４、更新ＳＱＬ文作成ステップ１２０５およびデータベース登録ステップ１２０６からなる。更新データ入力ステップ１２００では、ユーザがクライアント１００から入力した更新前のデータと更新後のデータを読み込む。更新前データ探索ステップ１２０１では、更新前のデータを管理テーブル１０７から検索する。一致デー

タチェックステップ１２０２では、更新前データ探索ステップ１２０１で検索した結果を判定する。更新前データ探索ステップ１２０１で検索した更新前データが管理テーブル１０７にない場合、更新処理を終了する。

【００４０】更新前データ探索ステップ１２０１で検索した更新前データが管理テーブル１０７にある場合、シリアル番号取得ステップ１２０３に進む。シリアル番号取得ステップでは、更新前データ探索ステップ１２０１で検索した更新前データのシリアル番号を取得する。更新後データ暗号化ステップ１２０４では、更新後のデータのハッシュ値を計算した後、更新後のデータをデータ暗号鍵で暗号化する。データ暗号鍵を鍵暗号鍵で暗号化する。更新ＳＱＬ文作成ステップ１２０５では、シリアル番号取得ステップ１２０３で取得したシリアル番号と更新後データ暗号化ステップ１２０４で作成した暗号化した更新後のデータを使って、更新するデータのＳＱＬ文を作成する。データベース登録ステップ１２０６では、データベース管理プログラム１１０により管理テーブル１０７のデータを更新実行プログラム１２４が更新データＳＱＬ文作成ステップ１２０５で作成したＳＱＬ文を実行して更新し、鍵テーブル１０８の更新後のデータのハッシュ値と暗号化したデータ暗号鍵と、暗号化アルゴリズム識別子を更新する。

【００４１】次に、更新前データ探索ステップ１２０１の処理を図１３のフローチャートを使って詳細に説明する。更新前データ探索ステップ１２０１は、ハッシュ値計算ステップ１３００、暗号化検索条件作成ステップ１３０１、管理テーブル検索ステップ１３０２、および一致データチェックステップ１３０３からなる。ハッシュ値計算ステップ１３００では、検索条件作成プログラム１１５を起動し、更新前データのハッシュ値を計算する。暗号化検索条件作成ステップ１３０１では、検索条件作成プログラム１１５を起動して、鍵テーブル１０８を検索してハッシュ値に一致する暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出す。鍵暗号鍵でデータ暗号鍵を復号し、復号したデータ暗号鍵と、暗号化アルゴリズム１１６で検索条件を暗号化する。管理テーブル検索ステップ１３０２では、検索実行プログラムを起動し、暗号化検索条件作成ステップ１３０１で暗号化したＳＱＬ文で管理テーブル１０７を検索する。一致データチェックステップ１３０３では、管理テーブル１０７に暗号化検索条件作成ステップ１３０１で作成したＳＱＬ文の検索条件に一致するデータがあるかどうかを調べる。暗号化検索条件作成ステップ１３０１で作成したＳＱＬ文の検索条件に一致するデータがある場合は、終了する。

【００４２】暗号化検索条件作成ステップ１３０１で作成したＳＱＬ文の検索条件に一致するデータがない場合は、ハッシュ値に一致する別の暗号化されたデータ暗号鍵と暗号化アルゴリズム識別子を取り出す。暗号化されたデータ暗号鍵を鍵暗号鍵で復号し、復号したデータ暗号鍵と、前記暗号化アルゴリズム識別子に対応する暗号化アルゴリズムで検索条件を暗号化し、その暗号化した検索条件で再度管理テーブル１０７を検索する。

【００４３】次に、更新後データ暗号化ステップ１２０４の処理を図１４のフローチャートを使って詳細に説明する。更新後データ暗号化ステップ１２０４は、ハッシュ値計算ステップ１４００、暗号アルゴリズム決定ステップ１４０１、データ暗号化ステップ１４０２および鍵暗号化ステップ１４０３からなる。ハッシュ値計算ステップ１４００では、更新後のデータのハッシュ値を計算する。暗号アルゴリズム決定ステップ１４０１では、暗号化プログラム１２０が今回の暗号化に使用する暗号化アルゴリズムを決定する。暗号化プログラム１２０は複数の暗号アルゴリズムを持つことができ、その中で登録・更新時の暗号化にはもっとも新しく暗号化プログラム１２０に登録された暗号アルゴリズムを使用するようにしている。データ暗号ステップ１４０２では、データ暗号鍵を作成し、管理テーブル１０７に登録するデータを暗号化する。鍵暗号化ステップ１４０３では、データ暗号鍵を鍵格納エリア１２８にある鍵暗号鍵により暗号化する。

【００４４】図１５は、削除制御プログラム１１３が実行する暗号化データベースのデータの削除処理フローを示している。データ削除処理は、削除データ入力ステップ１５００、削除データ探索ステップ１５０１、一致データチェックステップ１５０２、シリアル番号取得ステップ１５０３、削除ＳＱＬ文作成ステップ１５０４およびデータベース削除実行ステップ１５０５からなる。削除データ入力ステップ１５００では、ユーザがクライアント１００から入力した削除するデータを読み込む。削除データ探索ステップ１５０１では、削除データを検索する。一致データチェックステップ１５０２では、削除データ探索ステップ１５０１で検索した削除データが管理テーブル１０７にあるかどうかチェックする。削除データ探索ステップ１５０１で検索した削除データが管理テーブル１０７にない場合、削除処理を終了する。

【００４５】削除データ探索ステップ１５０１で検索した削除データが管理テーブル１０７にある場合、シリアル番号取得ステップ１５０３に進む。シリアル番号取得ステップ１５０３では、削除データ探索ステップ１５０１で検索した削除データのシリアル番号を取得する。削除ＳＱＬ文作成ステップ１５０４では、シリアル番号取得ステップ１５０３で取得したシリアル番号を使って削除ＳＱＬ文を作成する。データベース削除実行ステップ１５０５では、削除ＳＱＬ文作成ステップ１５０４で作成した削除ＳＱＬ文を使って管理テーブル１０７と鍵テーブル１０８からシリアル番号取得ステップ１５０３で取得したシリアル番号の行を削除する。削除データ探索ステップ１５０１に戻り、処理を続ける。

【００４６】以上、本実施例の特徴として、管理テーブルとそのテーブルの特定の値の集合（フィールド、行、列など）に関する暗号化のための情報（暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値）をもつ鍵テーブルにより秘密情報を管理することを特徴とするデータベース構造、およびその構成におけるデータの登録処理、検索処理、更新処理、削除処理について説明した。本実施例によれば、前記データベース構造を用いて、データ登録または更新時に暗号鍵を動的に変更し、暗号化のための情報を管理テーブルと別管理することにより、暗号化されたデータベースの安全性を高めることができる。また、管理テーブルの特定の値の集合ごとに異なる暗号化アルゴリズムを使用することが可能となり、さらにデータベース稼動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことも可能である。よって本実施例を適用することにより、十分なデータベースの安全性を確保することができる。

【００４７】次に、本発明の第二の実施例について説明する。本実施例は図１に示した第一の実施例と同様の構成をとるが、検索時にもデータ暗号鍵を更新するようにした部分が第一の実施例と異なる。第二の実施例の検索方式について図１６を使って説明する。第二の実施例のデータ検索処理は、検索データ入力ステップ１６００、ハッシュ値計算ステップ１６０１、検索ＳＱＬ文作成ステップ１６０２、管理テーブル検索ステップ１６０３、管理テーブル一致データチェックステップ１６０４、鍵テーブル検索ステップ１６０５、鍵テーブル一致データチェックステップ１６０６、検索結果表示ステップ１６０７、シリアル番号取得ステップ１６０８、全データ復号ステップ１６０９、鍵テーブル登録ステップ１６１０および管理テーブル登録ステップ１６１１からなる。

【００４８】図１６の検索データ入力ステップ１６００から全データ復号ステップ１６０９までの処理は、図１０の検索データ入力ステップ１０００から全データ復号ステップ１００９までの処理にそれぞれ対応し、同じ処理を行う。鍵テーブル登録ステップ１６１０において、検索条件に一致したデータを暗号化するためのデータ暗号鍵を新たに作成し、そのデータ暗号鍵を鍵暗号鍵で暗号化して、シリアル番号、暗号化アルゴリズム識別子とともに鍵テーブル１０８に登録する。管理テーブル登録ステップ１６１１において、鍵テーブル登録ステップ１６１０で作成したデータ暗号鍵を使って検索条件に一致したデータを暗号化して管理テーブル１０７に登録したあと、管理テーブル検索ステップ１６０３に戻って管理テーブル１０７の検索を続ける。

【００４９】以上、第二の実施例として、データ登録または更新時だけではなく検索時にも暗号鍵を変更する方式について説明した。本実施例によれば、前記データベース構造を用いて、データ登録、更新または検索時に暗号鍵を動的に変更することにより、第一の実施例のデータ登録または更新のときよりも頻繁に暗号鍵を更新するため暗号化されたデータベースの安全性をさらに高めることができる。

【００５０】次に、本発明の第三の実施例について説明する。第一の実施例では、新しい暗号化アルゴリズムが追加された場合に直ちにそれを使用していた。本実施例は図１に示した第一の実施例と同様の構成をとるが、暗号化アルゴリズムを上位で指定し、指定された暗号化アルゴリズムで暗号化するようにした部分が第一の実施例と異なる。

【００５１】図１を使って本実施例について説明する。データベースに暗号化して格納するデータの登録処理の概略について説明する。ユーザがクライアント１００からデータベースに登録するデータを入力し、暗号化アルゴリズム識別子を指定する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力された登録するデータと指定された暗号化アルゴリズム識別子が登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、登録・更新準備プログラム１１７に登録するデータと暗号化アルゴリズム識別子を渡す。登録・更新準備プログラム１１７は、初期条件作成プログラム１１８によりシリアル番号を作成し、ハッシュ値計算プログラム１１９により登録するデータのハッシュを計算し、暗号化プログラム１２０によりクライアント１００で指定された暗号化アルゴリズム識別子に基づくデータ暗号鍵を作成して、この鍵を使用して登録するデータを暗号化し、さらにそのデータ暗号鍵を鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより鍵格納エリア１２８にある鍵暗号鍵で暗号化する。

【００５２】登録・更新準備プログラム１１７は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、データ暗号鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、これらのデータを登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を登録実行プログラム１２３に渡す。登録実行プログラム１２３は、データベース管理プログラム１１０を使って管理テーブル１０７に、シリアル番号、暗号化された登録データを登録し、鍵テーブル１０８に、シリアル番号、登録されるデータのハッシュ値、データ暗号鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録する。

【００５３】次に、第三の実施例における、データの更新処理の概略について説明する。ユーザがクライアント

１００から更新前のデータ、更新後のデータ、および更新後のデータの暗号アルゴリズム識別子を指定する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力されたパラメータが登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、更新前のデータをデータ探索プログラム１１４に渡す。データ探索プラグラム１１４は、検索条件作成プログラム１１５により更新前のデータを暗号化し、検索実行プログラムにより更新前のデータのシリアル番号を取り出し、登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータ、更新後のデータを暗号化する暗号化アルゴリズム識別子を登録・更新準備プログラム１１７に渡す。

【００５４】登録・更新準備プログラム１１７は、ハッシュ値計算プログラムにより、更新後のデータのハッシュ値を計算し、暗号化プログラム１２０によりクライアント１００で指定された更新後のデータを暗号化する暗号化アルゴリズムに基づくデータ暗号鍵を作成して、更新するデータを暗号化し、さらに鍵暗号化プログラム１２１が、そのデータ暗号鍵を鍵格納エリア１２８にある鍵で鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより暗号化する。登録・更新準備プログラム１１７は、更新後のデータのハッシュ値、暗号化されたデータ、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータのハッシュ値、暗号化されたデータ、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を更新実行プログラム１２４に渡す。更新実行プログラム１２４は、データベース管理プログラム１１０を使って、管理テーブル１０７のデータと鍵テーブル１０８のデータのハッシュ値、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を更新する。

【００５５】以上で説明したように、第三の実施例によれば、上位アプリケーションが、自由に暗号化アルゴリズムを指定することができ、柔軟に暗号化アルゴリズムを選択することができる。

【００５６】以上、本発明の特徴として、管理テーブルとそのテーブルの特定のデータ集合（フィールド、行、列など）に関する暗号化のための情報（暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値）をもつ鍵テーブルにより秘密情報を管理することを特徴とするデータベース構造、その構成における暗号化されたデータの登録、検索、更新、削除、暗号鍵の動的な更新方法、およびデータベース稼動中の暗号化アルゴリズムの切り替え方法について説明した。本発明が用いるデータベース管理システムとしては、リレーショナルデータベースおよびオブジェクト指向データベースのいずれでも実施可能である。

【００５７】オブジェクト指向データベースを利用する場合には、鍵テーブル１０８の定義にオブジェクトを利用することになる。また、鍵テーブル１０８に、ハッシュアルゴリズムのフィールドを追加して、ハッシュアルゴリズムを暗号化アルゴリズムとともに特定のデータ集合ごとに変更することもできる。

【００５８】本発明によれば、前記データベース構造を用いて、暗号鍵を動的に変更し、暗号化のための情報を管理テーブルと別管理することにより、暗号化されたデータベースの安全性を高めることができる。また、特定のデータ集合ごとに新しい暗号化アルゴリズムに変更することが可能となり、データベース稼動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことも可能である。よって本発明を適用することにより、十分なデータベースの安全性を確保することができる。さらに将来より強固な暗号化アルゴリズムが発明された場合にも、管理データ暗号用のアルゴリズムを動的により強固な方式に切り替えていくことができる。

【００５９】

【発明の効果】本発明によれば、暗号化されたデータベースにおいて、データベース稼働中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことができ、柔軟性を持つ安全な秘密情報管理データベースを作成することができる。

【図面の簡単な説明】

【図１】本発明のデータベースの秘密情報管理方式の実施の一形態の構成を示す図である。

【図２】フィールドごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図３】フィールドごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図４】行ごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図５】行ごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図６】列ごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図７】列ごとに暗号化したデータベースの鍵テーブルを説明するための図である。

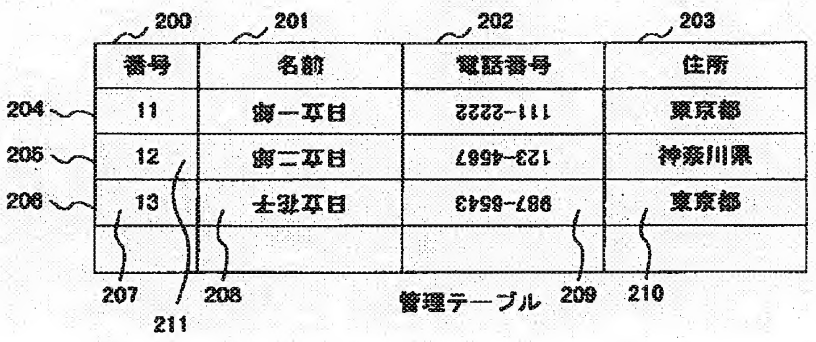
【図８】本発明により行われるデータベースのデータ登録の手順を説明するフローチャートである。

【図９】本発明により行われるデータベースのデータ登録時の登録・更新準備プログラムの手順を説明するフローチャートである。

【図１０】本発明により行われるデータベースのデータ検索の手順を説明するフローチャートである。
【図１１】本発明により行われるデータベースのデータ検索時の検索条件作成プログラムの手順を説明するフローチャートである。
【図１２】本発明により行われるデータベースのデータ更新の手順を説明するフローチャートである。
【図１３】本発明により行われるデータベースのデータ更新時のデータ探索プログラムの手順を説明するフローチャートである。
【図１４】本発明により行われるデータベースのデータ更新時の登録・更新準備プログラムの手順を説明するフローチャートである。
【図１５】本発明により行われるデータベースのデータ削除の手順を説明するフローチャートである。
【図１６】本発明により行われるデータベースの暗号鍵と暗号化アルゴリズムの変更を伴うデータ検索の手順を説明するフローチャートである。
【符号の説明】
１００　クライアント
１０１　ＬＡＮ
１０２　ＬＡＮアダプタ
１０３　サーバ
１０４　ＣＰＵ
＊１０５　バス
１０６　磁気ディスク装置
１０７　管理テーブル
１０８　鍵テーブル
１０９　主メモリ
１１０　データベース管理プログラム
１１１　登録・更新制御プログラム
１１２　検索制御プログラム
１１３　削除制御プログラム
１１４　データ探索プログラム
１１５　検索条件作成プログラム
１１６　検索実行プログラム
１１７　登録・更新準備プログラム
１１８　初期条件作成プログラム
１１９　ハッシュ値計算プログラム
１２０　暗号化プログラム
１２１　鍵暗号化プログラム
１２２　登録・更新条件作成プログラム
１２３　登録実行プログラム
１２４　更新実行プログラム
１２５　鍵取得プログラム
１２６　削除条件作成プログラム
１２７　削除実行プログラム
＊１２８　鍵格納エリア

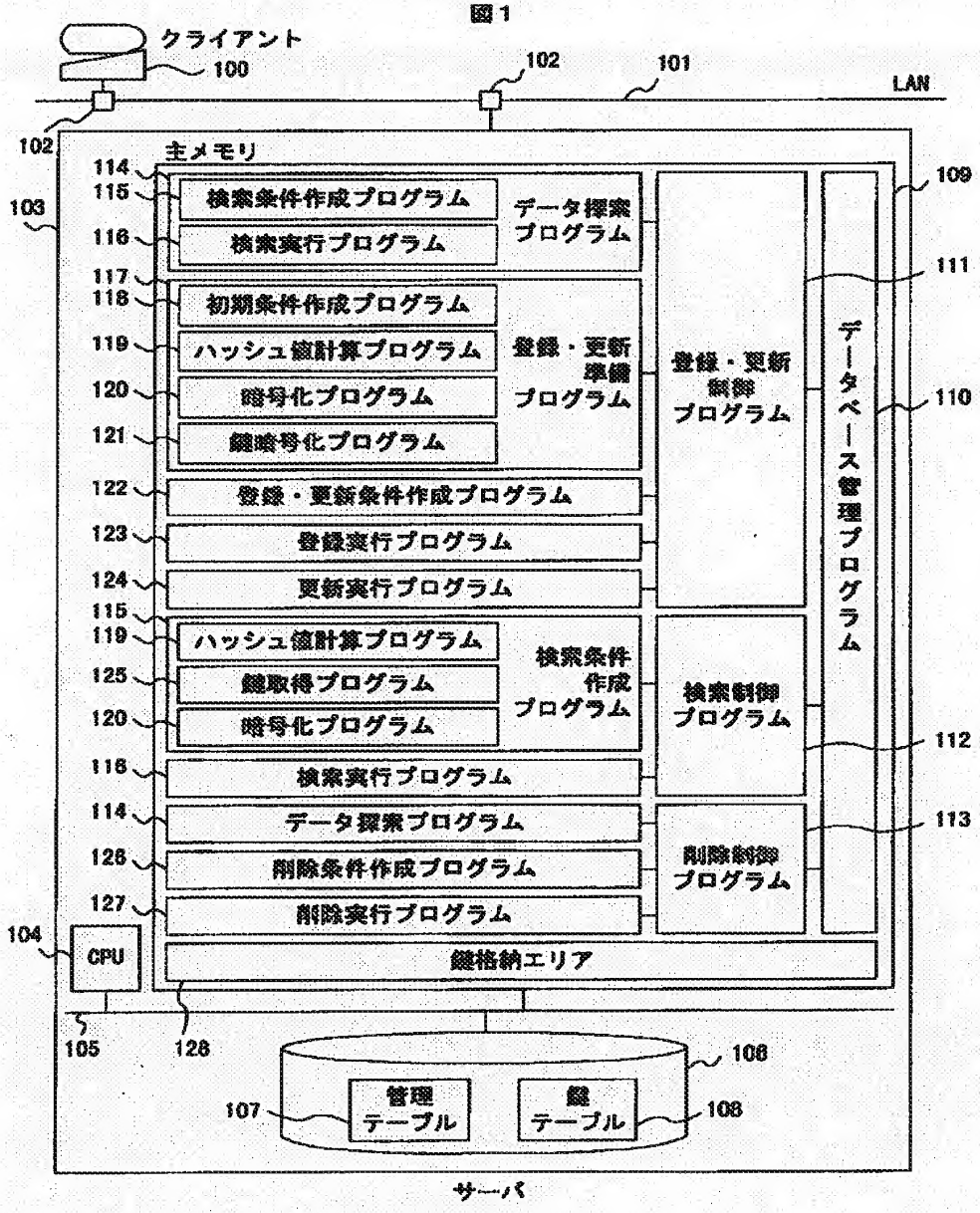
【図２】

図２



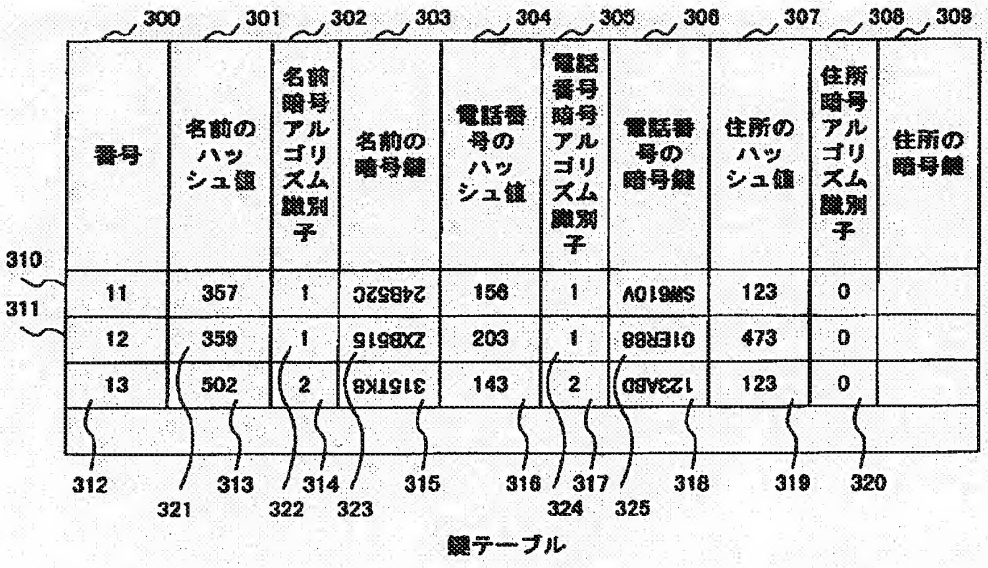
【図１】

図１


クライアント
100
102
101
LAN
102
主メモリ
114
115
検索条件作成プログラム
データ探索プログラム
103
116
検索実行プログラム
109
117
111
118
初期条件作成プログラム
119
ハッシュ値計算プログラム
登録・更新準備プログラム
登録・更新制御プログラム
データベース管理プログラム
120
暗号化プログラム
110
121
鍵暗号化プログラム
122
登録・更新条件作成プログラム
123
登録実行プログラム
124
更新実行プログラム
115
119
ハッシュ値計算プログラム
検索条件作成プログラム
検索制御プログラム
125
鍵取得プログラム
120
暗号化プログラム
112
116
検索実行プログラム
114
データ探索プログラム
113
126
削除条件作成プログラム
削除制御プログラム
127
削除実行プログラム
104
CPU
鍵格納エリア
105
128
106
107
管理テーブル
鍵テーブル
108
サーバ

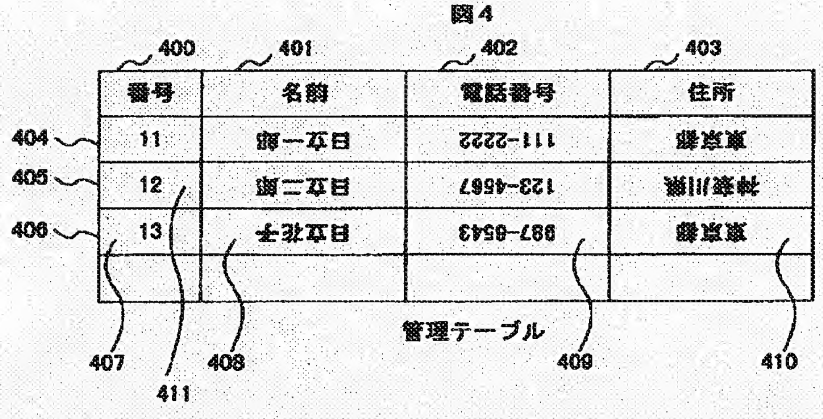
【図３】

図３


300
301
302
303
304
305
306
307
308
309
番号
名前のハッシュ値
名前暗号アルゴリズム識別子
名前の暗号鍵
電話番号のハッシュ値
電話番号暗号アルゴリズム識別子
電話番号の暗号鍵
住所のハッシュ値
住所暗号アルゴリズム識別子
住所の暗号鍵
310
311
11
357
1
248520
156
1
SM61OV
123
0
12
359
1
ZXB515
203
1
01ER88
473
0
13
502
2
315TK8
143
2
123ABD
123
0
312
321
313
322
314
323
315
316
324
317
325
318
319
320
鍵テーブル

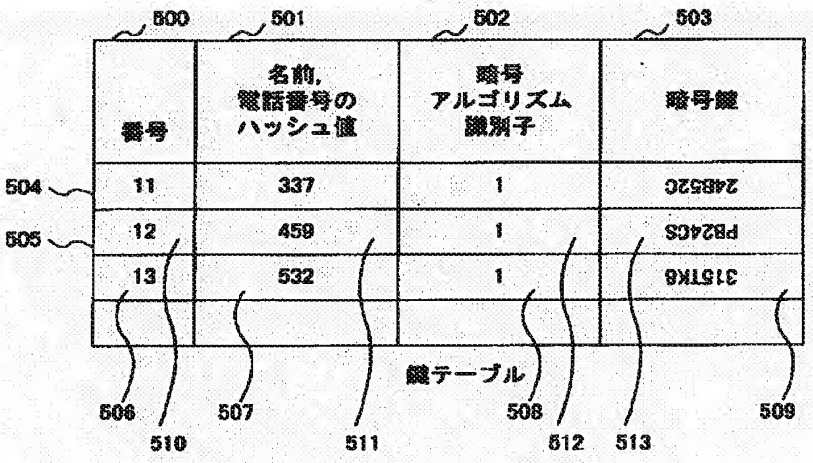
【図４】

図４


400
401
402
403
番号
名前
電話番号
住所
404
11
日立一郎
111-2222
東京都
405
12
日立二郎
123-4567
神奈川県
406
13
日立花子
987-6543
東京都
407
411
408
409
410
管理テーブル

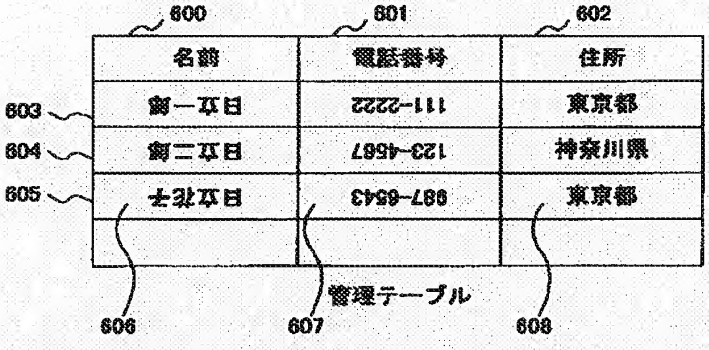
【図5】

図5



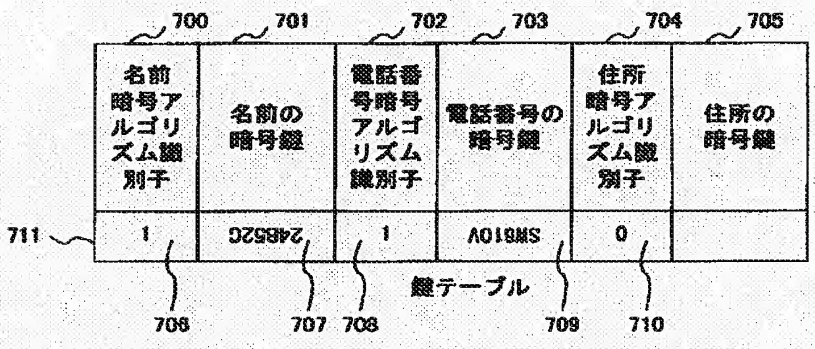
【図6】

図6



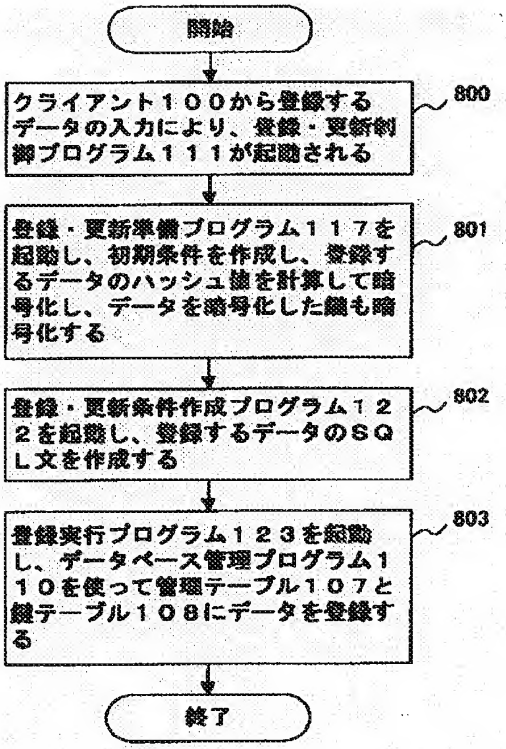
【図7】

図7



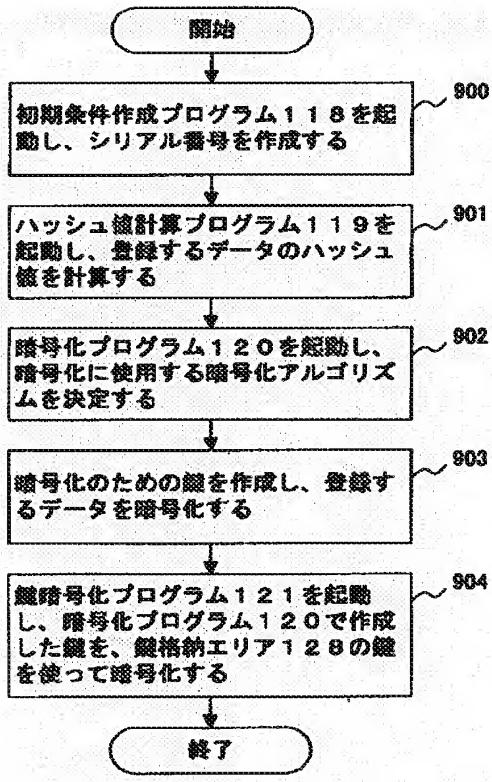
【図８】

図８



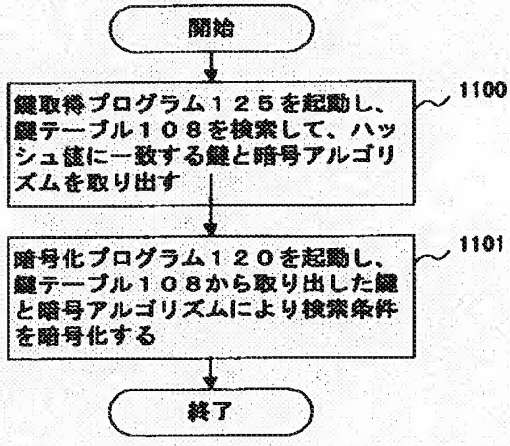
【図９】

図９



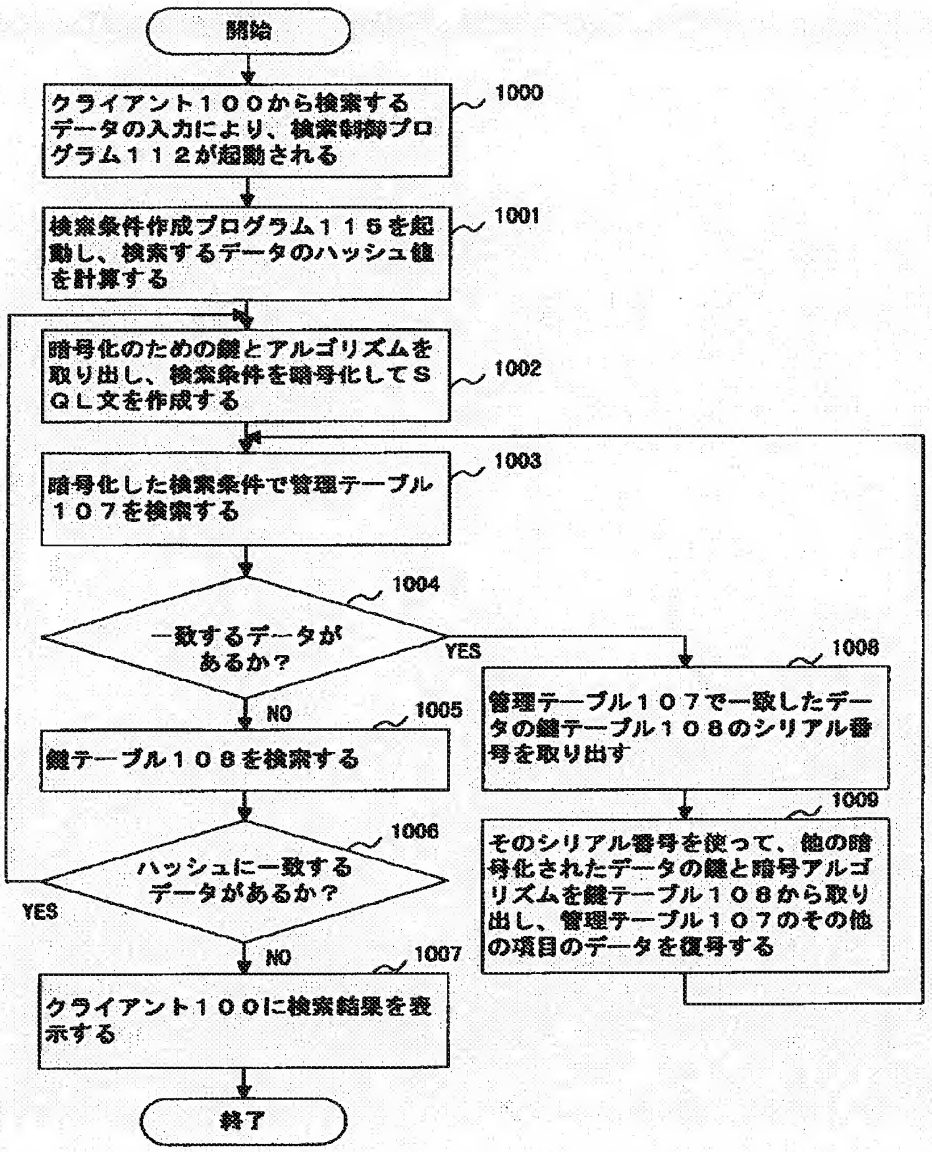
【図１１】

図１１



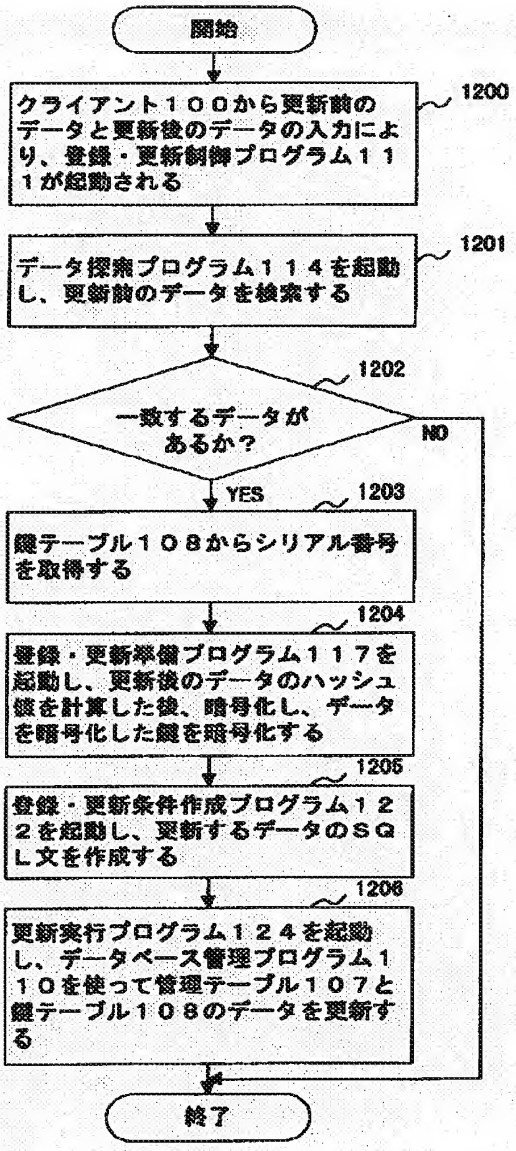
【図１０】

図１０


開始
クライアント１００から検索するデータの入力により、検索制御プログラム１１２が起動される
1000
検索条件作成プログラム１１５を起動し、検索するデータのハッシュ値を計算する
1001
暗号化のための鍵とアルゴリズムを取り出し、検索条件を暗号化してＳＱＬ文を作成する
1002
暗号化した検索条件で管理テーブル１０７を検索する
1003
一致するデータがあるか？
1004
YES
NO
管理テーブル１０７で一致したデータの鍵テーブル１０８のシリアル番号を取り出す
1008
鍵テーブル１０８を検索する
1005
そのシリアル番号を使って、他の暗号化されたデータの鍵と暗号アルゴリズムを鍵テーブル１０８から取り出し、管理テーブル１０７のその他の項目のデータを復号する
1009
ハッシュに一致するデータがあるか？
1006
YES
NO
クライアント１００に検索結果を表示する
1007
終了

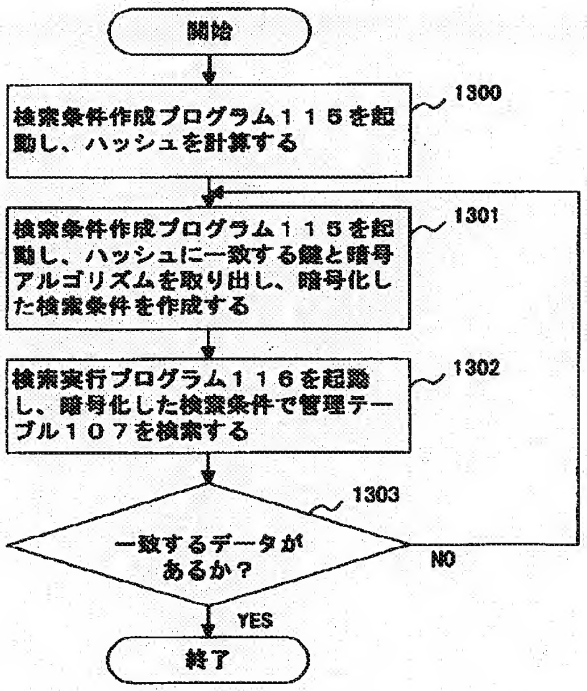
【図１２】

図１２



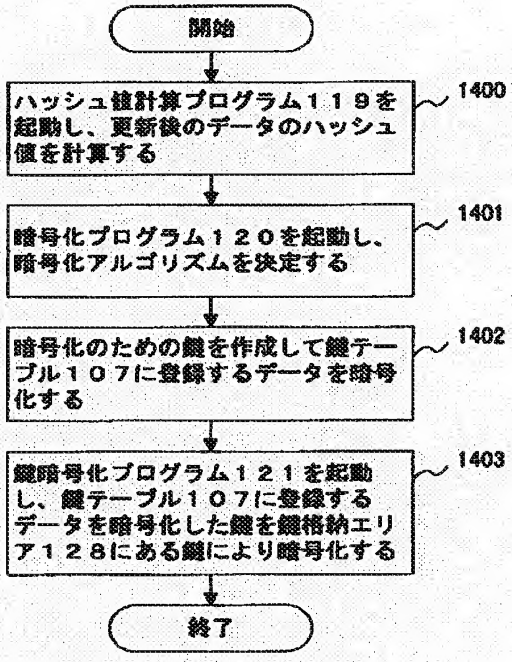
【図１３】

図１３



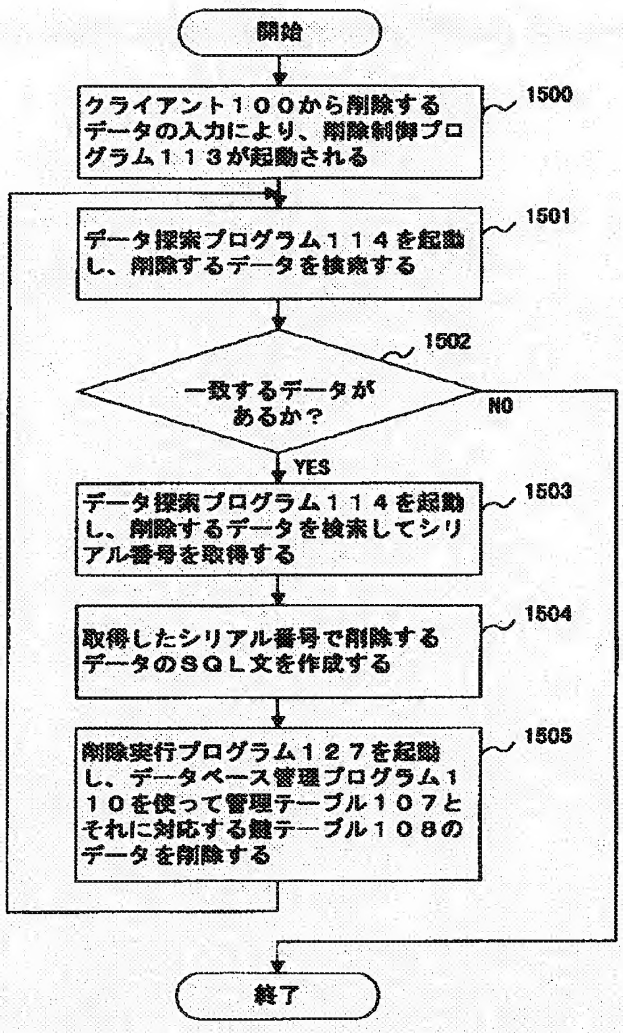
【図１４】

図１４



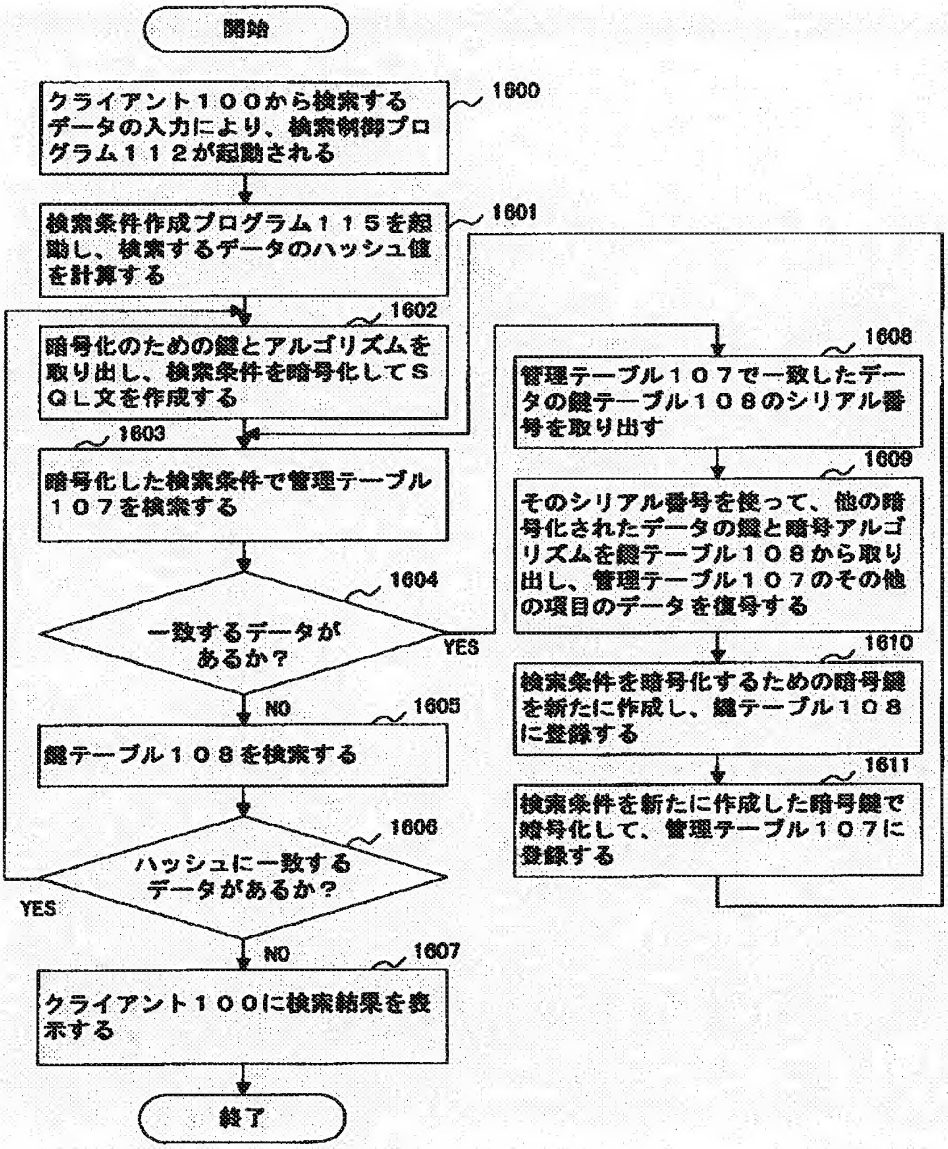
【図１５】

図１５


開始
クライアント１００から削除するデータの入力により、削除制御プログラム１１３が起動される
1500
データ探索プログラム１１４を起動し、削除するデータを検索する
1501
一致するデータがあるか？
1502
NO
YES
データ探索プログラム１１４を起動し、削除するデータを検索してシリアル番号を取得する
1503
取得したシリアル番号で削除するデータのＳＱＬ文を作成する
1504
削除実行プログラム１２７を起動し、データベース管理プログラム１１０を使って管理テーブル１０７とそれに対応する鍵テーブル１０８のデータを削除する
1505
終了

【図１６】

図１６


開始
クライアント１００から検索するデータの入力により、検索制御プログラム１１２が起動される
1600
検索条件作成プログラム１１５を起動し、検索するデータのハッシュ値を計算する
1601
暗号化のための鍵とアルゴリズムを取り出し、検索条件を暗号化してＳＱＬ文を作成する
1602
暗号化した検索条件で管理テーブル１０７を検索する
1603
一致するデータがあるか？
1604
YES
NO
鍵テーブル１０８を検索する
1605
ハッシュに一致するデータがあるか？
1606
YES
NO
クライアント１００に検索結果を表示する
1607
終了
管理テーブル１０７で一致したデータの鍵テーブル１０８のシリアル番号を取り出す
1608
そのシリアル番号を使って、他の暗号化されたデータの鍵と暗号アルゴリズムを鍵テーブル１０８から取り出し、管理テーブル１０７のその他の項目のデータを復号する
1609
検索条件を暗号化するための暗号鍵を新たに作成し、鍵テーブル１０８に登録する
1610
検索条件を新たに作成した暗号鍵で暗号化して、管理テーブル１０７に登録する
1611

CLAIMS

[Claim(s)]
[Claim 1]A management table which stores confidential information which is a confidential information controlling method in a database which manages enciphered confidential information, and was enciphered by said database, a set (an item of one sequence in one line.) of a specific value of this management table A key table which stores a hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked is provided, Give a serial number to this management table and a key table for every line, and it relates with them mutually, A serial number is created at the time of registration of confidential information to said database, Confidential information which creates a key for enciphering confidential information to register using a random number, and registers it into said management table with a this created key is enciphered using a cryptographic algorithm, Enciphered this confidential information is registered into said management table with said serial number, Said hash value which is enciphered with a key encryption key used for encryption of all the keys which enciphered confidential information which is the key created apart from a this created key, and registers said created key into a management table, and is used for search of enciphered confidential information is calculated, A confidential information controlling method in a database registering into said key table a key for encryption of confidential information enciphered by this key encryption key, an identifier of said cryptographic algorithm, and a hash value for said search with said serial number.

[Claim 2]In the confidential information controlling method according to claim 1, at the time of search of confidential information registered into said database. Calculate a hash value of a search condition and a condition coincidence line which has a hash value which is in agreement with a hash value of this search condition is taken out from said key table, A key for encryption of confidential information enciphered by said key encryption key and a group of an encryption algorithm identifier are taken out from this condition coincidence line, A key for encryption of confidential information enciphered by this taken-out key encryption key is decoded with this key encryption key, A confidential information controlling method in a database enciphering said search condition by a cryptographic algorithm corresponding to a this decoded key and said encryption algorithm identifier, and searching said management table according to a this enciphered search condition.

[Claim 3]After searching confidential information which is in agreement with a search condition in a confidential information controlling method in the database according to claim 2, The new key for enciphering searched this confidential information is created using a random number, Confidential information this searched with a created this key is newly enciphered using a cryptographic algorithm, enciphering a created this key with said key encryption key -- this -- a management table by newly enciphered confidential information, [update and] A confidential information controlling method in a database updating a key table by an identifier of the new key for encryption enciphered with said key encryption key, and said cryptographic algorithm.

[Claim 4]In a confidential information controlling method in the database according to claim 2, at the time of renewal of confidential information registered into said database. Input confidential information before updating, and confidential information after updating, and a database is searched by confidential information before updating, A serial number of said management table in which confidential information before renewal of this exists is acquired, A key for enciphering confidential information after said updating is created using a random number, Confidential information after renewal of this is enciphered using a cryptographic algorithm with a created this key, A key which registered confidential information after enciphered this updating into a line of said acquired serial number of said management table, enciphered said created key with said key encryption key, and was enciphered with this key encryption key, A confidential information controlling method in a database registering an identifier of said cryptographic algorithm into a line of said acquired serial number of said key table.

[Claim 5]A confidential information controlling device of a database which manages enciphered confidential information characterized by comprising the following.

A management table which stores enciphered confidential information in said database.
a set (an item of one sequence in one line.) of a specific value of this management table It has a key table which stores a hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked, A means to give a serial number to this management table and a key table for every line, to relate mutually, and to create a serial number at the time of registration of confidential information.
A means to encipher confidential information which creates a key for enciphering confidential information to register using a random number, and registers it into said management table with a this created key using a cryptographic algorithm.
A means to register enciphered this confidential information into said management table with said serial number, A means to encipher with a key encryption key used for encryption of all the keys which enciphered confidential information which is the key created apart from a this created key, and registers said created key into a management table, A means to calculate said hash value used for search of enciphered confidential information, A key for encryption of confidential information enciphered by this key encryption key, and an identifier of said cryptographic algorithm, A means to register a hash value for said search into said key table with said serial number, A means which calculates a hash value of a search condition at the time of search of confidential information, and takes out a condition coincidence line which has a hash value which is in agreement with a hash value of this search condition from said key table, A means which takes out a key for encryption of confidential information enciphered by said key encryption key, and a group of an encryption algorithm identifier from this condition coincidence line, A means to decode a key for encryption of confidential information enciphered by this taken-out key encryption key with this key encryption key, A means to encipher said search condition by a cryptographic algorithm corresponding to a this decoded key and said encryption algorithm identifier, and to search said management table according to a this enciphered search condition.

[Claim 6]A confidential information controlling device of the database according to claim 5 characterized by comprising the following.
A means to acquire a serial number of said management table which searches a database by confidential information before inputted updating at the time of renewal

of confidential information and in which confidential information before renewal of this exists.
A means to create a key for enciphering confidential information after inputted updating using a random number, and to encipher confidential information after renewal of this using a cryptographic algorithm with a this created key.
A means to register confidential information after enciphered this updating into a line of said acquired serial number of said management table.
A means to encipher said created key with said key encryption key, a key enciphered with this key encryption key, and a means to register an identifier of said cryptographic algorithm into a line of said acquired serial number of said key table.

[Claim 7]It is the recording medium which recorded enciphered confidential information and key information used for encryption and in which computer reading is possible, Said enciphered confidential information is recorded on a management table, and key information used for said encryption is recorded on a key table, and said management table, Consist of two or more lines and two or more sequences, it is recorded by group of confidential information enciphered by each line correspondence, and said key table, a set (an item of one sequence in one line.) of a value with said specific management table which consists of two or more lines and two or more sequences A hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked is recorded, A recording medium which recorded enciphered confidential information, wherein a serial number which associates a line of a management table and a line of a key table mutually is recorded on each line of said management table and a key table, and key information used for encryption and in which computer reading is possible.
[Claim 8]a set (an item of one sequence in one line.) of a specific value of a management table which stores enciphered confidential information, and this management table It has a key table which stores a hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked, It is the recording medium which recorded a confidential information control program which manages a database which gave a serial number for every line, was associated mutually, and was used as this management table and a key table and in which computer reading is

possible, A procedure which creates a serial number at the time of registration of confidential information to said database, A procedure which enciphers confidential information which creates a key for enciphering confidential information to register using a random number, and registers it into said management table with a this created key using a cryptographic algorithm, A procedure of registering enciphered this confidential information into said management table with said serial number, A procedure enciphered with a key encryption key used for encryption of all the keys which enciphered confidential information which is the key created apart from a this created key, and registers said created key into a management table, and a procedure which calculates said hash value used for search of enciphered confidential information, A recording medium which recorded a confidential information control program which performs a procedure of registering into said key table a key for encryption of confidential information enciphered by this key encryption key, an identifier of said cryptographic algorithm, and a hash value for said search with said serial number and in which computer reading is possible.

[Claim 9]a set (an item of one sequence in one line.) of a specific value of a management table which stores enciphered confidential information, and this management table It has a key table which stores a hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked, It is the recording medium which recorded a confidential information control program which manages a database which gave a serial number for every line, was associated mutually, and was used as this management table and a key table and in which computer reading is possible, A procedure which calculates a hash value of a search condition at the time of search of confidential information to said database, and takes out a condition coincidence line which has a hash value which is in agreement with a hash value of this search condition from said key table, A procedure which takes out a key for encryption of confidential information enciphered by a key encryption key used for encryption of all the keys which enciphered confidential information, and a group of an encryption algorithm identifier from this condition coincidence line, Said search condition is enciphered by a cryptographic algorithm corresponding to a procedure which decodes a key for encryption of confidential information enciphered by this taken-out key encryption key with this key encryption key, a this decoded key, and said encryption algorithm identifier, A recording medium which recorded a confidential information control program which performs a procedure of searching said

management table according to an enciphered this search condition and in which computer reading is possible.
[Claim 10]a set (an item of one sequence in one line.) of a specific value of a management table which stores enciphered confidential information, and this management table It has a key table which stores a hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked, It is the recording medium which recorded a confidential information control program which manages a database which gave a serial number for every line, was associated mutually, and was used as this management table and a key table and in which computer reading is possible, A procedure which acquires a serial number of said management table which searches a database by confidential information before inputted updating at the time of renewal of confidential information registered into said database, and in which confidential information before renewal of this exists, A procedure which creates a key for enciphering confidential information after inputted updating using a random number, and enciphers confidential information after renewal of this using a cryptographic algorithm with a this created key, A procedure of registering confidential information after enciphered this updating into a line of said acquired serial number of said management table, and a procedure enciphered with a key encryption key which uses said created key for encryption of all the keys which enciphered confidential information, A recording medium which recorded a confidential information control program which performs a key enciphered with this key encryption key, and a procedure of registering an identifier of said cryptographic algorithm into a line of said acquired serial number of said key table and in which computer reading is possible.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the method of enciphering in a

database, registering confidential information and managing it.

[0002]

[Description of the Prior Art]The database is used in various fields, such as a credit company and a bank, these days. The certificate authority which especially attests electronic commerce technology these days also has a database which manages the confidential information of individuals, such as a name and a credit number, for attestation. Since such a database is treating the confidential information about an individual, it has prevented disclosure of data by making it not grant only a specific individual like a database administrator the right to access which can operate a database, for example. However, even when the right to access to a database is set up, an inaccurate invader carries out unjustly the memory storage which recorded the database, and there is a danger that data will be revealed, by seeing the contents of this device directly. Then, it is possible by enciphering and registering specific information, including a name, a credit number, etc., decoding, when taking out information, and acquiring the original information to secure security. Thus, if the key for decoding is not stolen even if the device with which the database was recorded by enciphering specific information suits a theft, the danger that information will be revealed decreases substantially. Conventionally, the whole database was enciphered using one specific key to encryption of such information.

[0003]There are some which are indicated by "JP,8-329011,A" as an example of the art which enciphers a database. The example of this well-known example comprises a network system which connects a database, a lock management center, 1 next user, and 2 next users mutually. 1 next user enciphers copyright information, stores in a database, and stores a key in a lock management center. When 2 next users use the copyright information, an encryption key is got from a lock management center, and the method then charged is proposed. The lock management center of this well-known example has managed the key by performing matching of the key currently kept and a copyright label.

[0004]

[Problem(s) to be Solved by the Invention]At a Prior art, in the database which enciphered the whole database with one specific encryption key, when the encryption key suits a theft simultaneously with the device with which the database was recorded, the whole database is decoded and there is a danger that confidential information will be revealed. When an encryption key suits a theft during operation of a database, an unauthorized entry person may decode data using this key. Therefore, it will be necessary to change an encryption key in these situations and to prevent

disclosure of data. In order to change an encryption key, access from the user to a database is forbidden, and once decrypting all the data in a database, it must reencipher with a new encryption key. The more the scale of a database becomes large, this work takes time and, the more the user cannot access a database in the meantime. Since the number of the keys which have enciphered the database is one when one of the data enciphered even if a key furthermore did not meet a theft is decoded, there is a danger that all other data will be decoded.

[0005]In a Prior art, when a firmer encryption algorithm tends to be adopted and it is going to raise security during operation of a database, it is difficult to change an encryption algorithm. It is because user access to a database is once forbidden also in this case and all the data must be reenciphered by a new encryption algorithm. In the method which enciphers the conventional database as stated above, Since the number of the keys which encipher a database is one, when the key suits a theft, Even if there is a danger that all the databases enciphered with the key will be decoded, and confidential information will be revealed and the firm encryption algorithm was invented by in the enciphered database operation, there was a problem that it was difficult to change the encryption algorithm of a database into the method.

[0006]In the method which enciphers a database, this invention provides the confidential information managing system of the safe database which does not reveal the contents of the database, It aims at enabling it to enable it to make a change of an encryption key or an encryption algorithm easily also during database operation, and to use two or more encryption algorithms and two or more encryption keys.

[0007]

[Means for Solving the Problem]A management table which stores confidential information which this invention is a confidential information controlling method in a database which manages enciphered confidential information, and was enciphered by said database in order to attain the above-mentioned purpose, a set (an item of one sequence in one line.) of a specific value of this management table A key table which stores a hash value of this set for which set correspondence of a specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked is provided, Give a serial number to this management table and a key table for every line, and it relates with them mutually, A serial number is created at the time of registration of confidential information to said database, Confidential information which creates a key for enciphering confidential information to register using a random number, and registers it into said management table with a this

created key is enciphered using a cryptographic algorithm, Enciphered this confidential information is registered into said management table with said serial number, Said hash value which is enciphered with a key encryption key used for encryption of all the keys which enciphered confidential information which is the key created apart from a this created key, and registers said created key into a management table, and is used for search of enciphered confidential information is calculated, He is trying to register into said key table a key for encryption of confidential information enciphered by this key encryption key, an identifier of said cryptographic algorithm, and a hash value for said search with said serial number.

[0008]A hash value of a search condition is calculated at the time of search of confidential information registered into said database, A condition coincidence line which has a hash value which is in agreement with a hash value of this search condition is taken out from said key table, A key for encryption of confidential information enciphered by said key encryption key and a group of an encryption algorithm identifier are taken out from this condition coincidence line, A key for encryption of confidential information enciphered by this taken-out key encryption key is decoded with this key encryption key, Said search condition is enciphered by a cryptographic algorithm corresponding to a this decoded key and said encryption algorithm identifier, and it is made to search said management table according to a this enciphered search condition.

[0009]After searching confidential information which is in agreement with a search condition, the new key for enciphering this searched confidential information is created using a random number, Confidential information this searched with a created this key is newly enciphered using a cryptographic algorithm, enciphering a created this key with said key encryption key -- this -- he updates a management table by newly enciphered confidential information, and is trying to update a key table by an identifier of the new key for encryption enciphered with said key encryption key, and said cryptographic algorithm

[0010]Confidential information before updating and confidential information after updating are inputted at the time of renewal of confidential information registered into said database, Search a database by confidential information before updating, and a serial number of said management table in which confidential information before renewal of this exists is acquired, A key for enciphering confidential information after said updating is created using a random number, Confidential information after renewal of this is enciphered using a cryptographic algorithm with a created this key, A key which registered confidential information after enciphered this updating into a

line of said acquired serial number of said management table, enciphered said created key with said key encryption key, and was enciphered with this key encryption key, He is trying to register an identifier of said cryptographic algorithm into a line of said acquired serial number of said key table.

[0011]

[Embodiment of the Invention]First, the principle of this invention is explained. The item of one sequence in one line of a management table and a management table for the database which manages confidential information to store the enciphered confidential information (below) It has the key used in order to encipher each value which belongs to this set for every set of specific values called the field, such as a line or a sequence, and a key table which stores an encryption algorithm identifier. Said management table and the key table store the serial number which associates the line of two tables, respectively, and the hash value calculated to the value which combined the set of the specific value of said management table is also stored in a key table. In registration of the enciphered confidential information, the key (below, a data encryption key is called) for enciphering confidential information is first created using a random number. The confidential information registered into a management table using the data encryption key is enciphered. There are MULTI2, DES (Data Encryption Standard), etc. as an example of such a key. Said data encryption key is enciphered using another key (below, a key encryption key is called) used for encryption of all the keys which enciphered the confidential information which is the key created apart from the key which enciphers confidential information, and is registered into a management table. And it calculates from the confidential information before enciphering the hash value used for search of confidential information. A serial number is generated, the confidential information enciphered as the serial number is registered into a management table, and a serial number, a data encryption key, an encryption algorithm identifier, and a hash value are registered into a key table.

[0012]When a serial number is specified as a search condition, the serial number is searched in a key table, the data encryption key enciphered as the encryption algorithm identifier which is in agreement with the serial number is picked out from a key table, and the data encryption key enciphered with the key encryption key is decoded. Next, a serial number is searched in a management table, the enciphered confidential information which is in agreement with a serial number is taken out from a management table, and the confidential information is decoded using said data encryption key by said cryptographic algorithm. When only confidential information is specified as a search condition, the hash value of a search condition is calculated first.

A search condition is enciphered as the enciphered data encryption key which searches a key table by the hash value, and is in agreement with the hash value, and the data encryption key which took out all encryption algorithm identifiers and decoded said enciphered data encryption key by an encryption algorithm. Next, a management table is searched using the enciphered search condition, and when the line containing confidential information in agreement is found, confidential information other than a search condition is decoded using the key and encryption algorithm identifier which decoded the enciphered data encryption key of everything but the key table corresponding to the serial number of the line.

[0013]The principle explained above is further explained using an example. The example of the management table used by this example is shown in drawing 2, and the key table corresponding to the management table is shown in drawing 3. The sequence of a management table is constituted and in a serial number, a name, a telephone number, and an address the sequence of a key table, It comprises an encryption key of a serial number, the hash value of a name, a name encryption algorithm identifier, the encryption key of a name, the hash value of a telephone number, a telephone number encryption algorithm identifier, the encryption key of a telephone number, the hash value of an address, an address encryption algorithm identifier, and an address. In drawing 2 and drawing 3, the character of top-and-bottom reverse shows the data enciphered. It is stored in the management table of drawing 2 without enciphering a name and a telephone number and enciphering an address. A name, a telephone number, each hash value of an address, an encryption algorithm identifier, and an encryption key are stored in the key table of drawing 3, among these the encryption key is enciphered and stored in it.

[0014]By this example, the line 205 of "12" is stored [the sequence of the item 200 of a serial number] in the management table for the sequence of the line 204 of "11", and the item 200 of a serial number, and the sequence of the item 300 of a serial number The "11" lines 310, A procedure in case the sequence of the item 300 of a serial number newly registers a name "day rikka child", a telephone number "987-6543", and the address "Tokyo" into a database in the state where the line 311 of "12" is stored in the key table 108 is explained. First, the key for enciphering a "day rikka child" and "987-6543" is created using a random number, respectively, and "315TK8" and "123ABD" are calculated. Next, it enciphers by the newest cryptographic algorithm in which an enciphered program has a "day rikka child" using the created key "315TK8", and "987-6543" is enciphered by said cryptographic algorithm using a key "123ABD." Next, the hash value "502" is calculated from a "day

rikka child", the hash value "143" is calculated from "987-6543", and the hash value "123" is calculated from "Tokyo." A key "315TK8" and "123ABD" are enciphered with a key encryption key. The serial number "13" which connects the line of a management table and a key table is generated, The "day rikka child" enciphered by the item 207 of the serial number of a management table at the item 208 of "13" and a name, "Tokyo" is registered into the item 210 of "987-6543" and an address enciphered by the item 209 of the telephone number, In the item 312 of the serial number of a key table at the item 313 of the hash value of "13" and a name "502", "315TK8" enciphered by the item 314 of the encryption algorithm identifier of a name at the item 315 of the encryption key of "2" and a name, In the item 316 of the hash value of a telephone number at the item 317 of "143" and the encryption algorithm identifier of a telephone number "2", "0" is registered into the item 319 of the hash value of "123ABD" enciphered by the item 318 of the encryption key of a telephone number, and an address at the item 320 of "123" and the encryption algorithm identifier of an address.

[0015]Next, the case where a name searches the telephone number of "Hitachi 2 **" is explained from this confidential information database (a management table and a key table). First, a hash value is calculated from "Hitachi 2 **", and the hash value "359" is calculated. "359" is searched with the hash value of the name of a key table, and data encryption key "ZXB515" 323 enciphered as the encryption algorithm identifier "1" 322 are taken out. Next, a data encryption key is decoded with a key encryption key. Decoded encryption key "ZXB515" The search condition "Hitachi 2 **" of a name is enciphered as 323 using encryption algorithm identifier "1" 322. A management table is searched using the search condition of enciphered "Hitachi 2 **." Search "Hitachi 2 **" enciphered in the management table, and serial number "12" 211 of the line are taken out, The serial number "12" The telephone number as which "Hitachi 2 **" on a management table was enciphered using the key which decoded the data encryption key "01ER88" enciphered using 211 as encryption algorithm identifier "1" 324 of the telephone number of a key table with the key encryption key is decrypted.

[0016]Next, the case where a data encryption key which uses the same data encryption key for each of the value contained in each line, and is different for every line is used is explained. The example of the management table and key table in this case is shown in drawing 4 and drawing 5. Drawing 4 is an example of the management table enciphered for every line. Although the table format of drawing 4 is the same as drawing 2, unlike drawing 2, the unit enciphered and stored has become for every line.

In drawing 4, the character of top-and-bottom reverse shows the data enciphered. The example of the key table corresponding to the management table of drawing 4 is shown in drawing 5. The key table of drawing 5 has the hash value, encryption algorithm identifier, and data encryption key of the value which connected the serial number, and a name and a telephone number in a sequence. Since a key table has the key enciphered for every line, only a hash value, an encryption algorithm identifier, and one encryption key exist for every line. In drawing 5, the character of top-and-bottom reverse shows the data enciphered. The sequence 500 of the item of a serial number stores the serial number for associating the line of a management table and a key table. Although the name and the hash value calculated combining two of telephone numbers are stored in a name and the sequence 501 of the item of the hash value of a telephone number in drawing 5, it may be made for this to calculate a hash value from one only of the names. A database with the structure of the management table of drawing 4 and the key table of drawing 5 enables it to encipher with a respectively different data encryption key for every line.

[0017]By this example, the line 405 of "12" is stored [the sequence 400 of the item of a serial number] in the management table for the sequence 400 of the line 404 of "11", and the item of a serial number, and the sequence 500 of the item of a serial number The "11" lines 504, A procedure in case the sequence 500 of the item of a serial number newly registers a name "day rikka child", a telephone number "987-6543", and the address "Tokyo" into a database in the state where the line 505 of "12" is stored in the key table is explained. First, the key for enciphering a "day rikka child", "987-6543", and "Tokyo" is created one using a random number, and "315TK8" is calculated. Next, it enciphers by the newest cryptographic algorithm in which an enciphered program has a "day rikka child", "987-6543", and "Tokyo" using the created key "315TK8", respectively. Next, the hash value "532" is calculated from a "day rikka child" and "987-6543." The key "315TK8" is enciphered with a key encryption key. The serial number "13" which connects the line of a management table and a key table is generated, The "day rikka child" enciphered by the item 407 of the serial number of a management table at the item 408 of "13" and a name, "987-6543" enciphered by the item 409 of the telephone number and "Tokyo" enciphered by the item 410 of the address are registered, "315TK8" which was enciphered by the item 506 of the serial number of a key table at the item 507 of the hash value of "13", a name, and a telephone number, and was enciphered by the item 508 of "532" and an encryption algorithm identifier at the item 509 of "1" and an encryption key is registered.

[0018]Next, a name explains the case where a telephone number searches the address of "123-4567" with "Hitachi 2 **" from this confidential information database (a management table and a key table). When retrieving the information enciphered in the database enciphered for every line, all the items used in order to calculate a hash value are specified in a search condition, and if they are practice ****, there are. [no] First, hash is calculated from "Hitachi 2 **" and "123-4567", and the hash value "459" is calculated. "459" is searched with the name of a key table, and the hash value of a telephone number, and the data encryption key "PB24CS" 513 enciphered as the encryption algorithm identifier "1" 512 is taken out. Next, a data encryption key is decoded with a key encryption key.
[0019]The search condition which enciphered "Hitachi 2 **" and "123-4567" as the taken-out encryption key "PB24CS" 513 using encryption algorithm identifier "1" 512 is created. A management table is searched using the enciphered search condition of "Hitachi 2 **" and "123-4567." If "Hitachi 2 **" enciphered in the management table and "123-4567" are searched and a line in agreement is shown in a management table, A serial number decrypts the address where the management table of the line of "12" was enciphered using the key and encryption algorithm which enciphered "Hitachi 2 **" and "123-4567."
[0020]The example of a management table and a key table in case the specific set to encipher is a sequence is shown in drawing 6 and drawing 7. It differs from drawing 2 in that the table format of drawing 6 does not have an item of a serial number. In drawing 6, the character of top-and-bottom reverse shows the data enciphered. In drawing 6, the data of the item 602 of an address is stored without being enciphered. The example of the key table corresponding to the management table of drawing 6 is shown in drawing 7. In drawing 7, the character of top-and-bottom reverse shows the data enciphered. Drawing 7 is an example of the key table in the case of using a data encryption key which uses the same data encryption key for each of the value contained in each sequence, and is different for every sequence. In this case, since all the lines use the same encryption key and encryption algorithm for every sequence, a hash value is not stored. With a database with the structure of the management table of drawing 6, and the key table of drawing 7, encryption of the database which has a respectively different encryption key for every sequence is attained.
[0021]By this example, the line 603 and the line 604 of the management table are stored in the management table, and the line 711 explains the procedure in the case of newly registering a name "day rikka child", a telephone number "987-6543", and the address "Tokyo" into a database in the state where it is stored in the key table. First,

the key for enciphering a "day rikka child" and "987-6543" is acquired. Therefore, "24B-52C" and "SW610V" which were enciphered with the key encryption key, an encryption algorithm identifier "1", and "1" are acquired from a key table, and "24B-52C" and "SW610V" which were enciphered with the key encryption key are decoded with a key encryption key. Next, it enciphers by the cryptographic algorithm which took out the "day rikka child" from the key table using the acquired key "24B-52C", and "987-6543" is enciphered by said encryption algorithm using a key "SW610V."

[0022]Next, the case where a name searches the telephone number of "Hitachi 2 **" is explained from this confidential information database (a management table and a key table). First, the data encryption key "24B-52C" 707 enciphered as encryption algorithm identifier "1" 706 of the name is picked out from a key table. Next, the enciphered data encryption key "24B-52C" is decoded with a key encryption key. The search condition "Hitachi 2 **" of a name is enciphered for said data encryption key "24B-52C" 707 using encryption algorithm identifier "1" 706. A management table is searched using the search condition of enciphered "Hitachi 2 **." The telephone number as which the line of "Hitachi 2 **" was enciphered is decrypted using what decrypted the encryption key "SW610V" 709 of the telephone number of a key table, and an encryption algorithm identifier "1."

[0023]As mentioned above, in the database which enciphers and registers confidential information, a set (the item of one sequence in one line.) of the specific value of the management table which stores the enciphered confidential information, and this management table By managing using two of key tables which stores the hash value of this set for which the set correspondence of the specific value of a key, an encryption algorithm identifier, and this management table used in order to encipher each value belonging to this set to correspondences, such as a line and a sequence, was asked, It becomes possible to change an encryption key and an encryption algorithm for every set of the specific value of a management table.

[0024]Hereafter, the first example of this invention is described using drawing 1. This system comprises the client 100, LAN101, LAN adapter 102, and the server 103. The client 100 and the server 103 are connected by LAN101 via LAN adapter 102. The server 103 comprises CPU104, the main memory 109, the bus 105, and the magnetic disk drive 106. The main memory 109 and the magnetic disk drive 106 are accessed via the bus 105 from CPU104. In the main memory 109. The database management program 110, registration and an update control program 111, the search control program 112, the deletion control program 113, the data search program 114,

registration / updating preparation program 117, registration and a renewal condition preparing program 122, the registration execution program 123, The updating execution program 124, the search condition preparing program 115, the retrieval execution program 116, the deletion-conditions preparing program 126, the deletion execution program 127, and the key storage area 128 are stored.

[0025]The data search program 114 comprises the search condition preparing program 115 and the retrieval execution program 116. Registration / updating preparation program 117 comprises the initial condition preparing program 118, the hash value calculation program 119, the enciphered program 120, and the key enciphered program 121. A search condition preparing program is hash value calculation program 119 and key acquisition programmed 125, and comprises the enciphered program 120. The management table 107 and the key table 108 are stored in the magnetic disk drive 106.

[0026]Hereafter, in the system of the composition of drawing 1, the outline of the registration processing of the data enciphered and stored in a database is explained. A user inputs the data registered into a database from the client 100. Registration and the update control program 111 are started, and the data which was inputted from the client 100 and to register is passed to registration and the update control program 111. Registration and the update control program 111 pass the data registered into registration / updating preparation program 117. Registration / updating preparation program 117 creates a serial number by the initial condition preparing program 118, Calculate hash of the data registered by the hash value calculation program 119, and the key which enciphers the data registered by the enciphered program 120 is created, The data registered by the newest encryption algorithm that the enciphered program 120 has is enciphered, and it enciphers with the key which is in the key storage area 128 by the encryption algorithm in which the key enciphered program 121 has a key to the encryption further. Registration / updating preparation program 117 passes the key which enciphered a serial number, the hash value of the data registered, the enciphered registration data, and the enciphered registration data, and the encryption algorithm identifier which enciphered registration data to registration and the update control program 111. Registration and the update control program 111 pass the key which enciphered a serial number, the hash value of the data registered, the enciphered registration data, and the enciphered registration data, and the encryption algorithm identifier which enciphered registration data to registration and the renewal condition preparing program 122. Registration and the renewal condition preparing program 122 create the SQL sentence for the management table 107 and the key

table 108 from the passed data, respectively, and passes it to registration and the update control program 111. Registration and the update control program 111 pass the SQL sentence created by registration and the renewal condition preparing program 122 to the registration execution program 123. The registration execution program 123 using the database management program 110 to the management table 107. A serial number and the enciphered registration data are registered and a serial number, the hash value of the data registered, the key that enciphered the enciphered registration data, and the encryption algorithm identifier which enciphered registration data are registered into the key table 108.

[0027]Next, in this system of such composition, the outline of the retrieval processing of the data which was enciphered and was registered into the database is explained. A user inputs the data searched from the client 100. The search control program 112 is started and the data which was inputted from the client 100 and to search is passed to the search control program 112. The search control program 112 passes the data searched to the search condition preparing program 115. The search condition preparing program 115 calculates the hash value of the data searched by the hash value calculation program 119, and takes out the encryption key with which the line which is in agreement with said hash value from the key table 108 by the key acquisition program 125 was enciphered, and an encryption algorithm identifier. The enciphered data encryption key is decoded with a key encryption key. A search condition is enciphered by the decoded data encryption key and encryption algorithm identifier, and the SQL sentence for search is created. The search condition preparing program 115 passes the created SQL sentence to the search control program 112. The search control program 112 passes said SQL sentence to the retrieval execution program 116. The retrieval execution program 116 searches the data which is in agreement with the search condition enciphered using the database management program 110 from the management table 107. The database management program 110 passes search results to the search control program 112. The search control program 112 returns the search results which decoded search results and were decoded to the client 100. The client 100 displays search results on a screen.

[0028]Next, in this system of such composition, the outline of the update process of the data which was enciphered and was stored in the database is explained. A user inputs the data before updating, and the data after updating from the client 100. Registration and the update control program 111 are started, and the data before updating inputted from the client 100 and the data after updating are passed to registration and the update control program 111. Registration and the update control

program 111 pass the data before updating to the data search program 114. The data search plug rum 114 enciphers the data before updating by the search condition preparing program 115, takes out the serial number of the data before updating by the retrieval execution program 116, and passes it to registration and the update control program 111. Registration and the update control program 111 pass the data after a serial number and updating to registration / updating preparation program 117. Registration / updating preparation program 117 by the hash value calculation program 119. Calculate the hash value of the data after updating and the key which enciphers the data after updating by the enciphered program 120 is created, It enciphers by the newest encryption algorithm in which the enciphered program 120 has data to update, and the key enciphered program 121 enciphers the key to the encryption further by the encryption algorithm which the key enciphered program 121 has with the key encryption key in the key storage area 128.

[0029]Registration / updating preparation program 117 passes the key which enciphered the hash value of the data after updating, the data after enciphered updating, and the data after enciphered updating, and the encryption algorithm identifier which enciphered the data after updating to registration and the update control program 111. Registration and the update control program 111 pass the key which enciphered a serial number, the hash value of the data after updating, the data after enciphered updating, and the data after enciphered updating, and the encryption algorithm identifier which enciphered the data after updating to registration and the renewal condition preparing program 122. Registration and the renewal condition preparing program 122 create the SQL sentence for the management table 107 and the key table 108 from the passed data, respectively, and passes it to registration and the update control program 111. Registration and the update control program 111 pass the SQL sentence created by registration and the renewal condition preparing program 122 to the updating execution program 124. The database management program 110 is used for the updating execution program 124, The key and encryption algorithm identifier which enciphered the hash value of the data after updating as which the management table 107 was enciphered, and the data after renewal of the key table 108, and the data after enciphered updating are updated according to a serial number.

[0030]Next, in this system of such composition, the outline of the deletion of the data which was enciphered and was stored in the database is explained. A user inputs the data deleted from the client 100. The deletion control program 113 is started and the data which was inputted from the client 100 and to delete is passed to this. The

deletion control program 113 passes the data to delete to the data search program 114. The data search program 114 enciphers the data deleted by the search condition preparing program 115, takes out the serial number of the data deleted by the retrieval execution program 116, and passes it to the deletion control program 113. The deletion control program 113 passes said serial number to the deletion-conditions preparing program 126. The deletion-conditions preparing program 126 creates the SQL sentence for the management table 107 and the key table 108 from the passed data, respectively, and passes it to the deletion control program 113. The deletion control program 113 passes the SQL sentence created by the deletion-conditions preparing program 126 to the deletion execution program 127. The deletion execution program 127 deletes the line of the serial number passed from the management table 107 and the key table 108 using the database management program 110.

[0031]Above-mentioned processing is explained still in detail using a flow chart. The following explanation explains the case where the management table of drawing 2 and the key table of drawing 3 are used as an example. Drawing 8 shows the registration processing flow of the data to the encryption database which registration / updating program 111 performs.

[0032]Data registration processing consists of the registration data input step 800, the registration preparation step 801, the registration data SQL sentence creation step 802, and the database register step 803. In the registration data input step 800, a user reads the data which was inputted from the client 100 and to register. In the registration preparation step 801, a serial number is created, the hash value of the data to register is calculated, the data encryption key which enciphers the data to register is created, and the data registered with the data encryption key is enciphered. A data encryption key is enciphered with a key encryption key. In the registration data SQL sentence creation step 802, the SQL sentence registered into the management table 107 and the key table 108 is created from the serial number created by the registration preparation step 801, the calculated hash value, the enciphered data encryption key, and the enciphered data to register. In the database register step 803, the SQL sentence which the registration execution program 123 created at the registration data SQL sentence creation step 802 is performed, The data which was enciphered by the management table 107 as the serial number by the database management program 110 and to register is registered, and the key and encryption algorithm identifier which enciphered the registration data enciphered as the hash value of a serial number and registration data to the key table 108 are registered.

[0033]Next, processing of the registration preparation step 801 is explained in detail

using the flow chart of drawing 9. The registration preparation step 801 consists of the serial number creation step 900, the hash value calculation steps 901, the cryptographic algorithm determination step 902, the data encryption step 903, and the key encryption step 904. In the serial number creation step 900, the serial number which connects each line of the management table 107 and the key table 108 is created. The hash value of the data to register is calculated in the hash value calculation steps 901. In the cryptographic algorithm determination step 902, the enciphered program 120 determines the encryption algorithm used for this encryption. The enciphered program 120 can have two or more cryptographic algorithms, and he is trying to use in it the cryptographic algorithm most newly registered into the enciphered program 120 for encryption at the time of registration and updating. In the data encryption step 903, the data encryption key for enciphering the data to register is created, and the data registered with the data encryption key is enciphered. In the key encryption step 904, the key created at the data encryption step 903 is enciphered using the key encryption key in the key storage area 128.

[0034]Drawing 10 shows the retrieval processing flow of the data to the encryption database which the search control program 112 performs. Data retrieval processing, The retrieved data input step 1000, the hash value calculation steps 1001, the search SQL sentence creation step 1002, the management table searching step 1003, the management table coincidence data check step 1004, the key table searching step 1005, It consists of the key table coincidence data check step 1006, the search-results displaying step 1007, the serial number acquisition step 1008, and all the data decryption steps 1009. In the retrieved data input step 1000, a user reads the data which was inputted from the client 100 and to search. The hash value of the data to search is calculated in the hash value calculation steps 1001. The data encryption key with which the line which is in agreement with the hash value calculated by the hash value calculation steps 1001 in the search SQL sentence creation step 1002 was enciphered, An encryption algorithm identifier is taken out from the key table 108 (the SQL sentence about a hash value is created and it takes out from a key table), a data encryption key is decoded, retrieved data is enciphered with the decoded data encryption key, and the SQL sentence which searches a management table is created. The management table 107 is searched with the management table searching step 1003 by the SQL sentence created at the search SQL sentence creation step 1002. In the management table coincidence data check step 1004, it is investigated whether the data which is in agreement with the SQL sentence created at the search SQL sentence creation step 1002 is shown in the management table 107. When the data

which is in agreement with the SQL sentence created at the search SQL sentence creation step 1002 is shown in the management table 107, it progresses to the serial number acquisition step 1008. In the serial number acquisition step 1008, the serial number of the key table 108 of data congruous with the management table 107 is taken out. The serial number taken out by the serial number acquisition step 1008 in all the data decryption steps 1009 to all the enciphered data encryption keys, An encryption algorithm identifier is taken out and all the data in which the management table was enciphered as the data encryption key decoded with the key encryption key by the encryption algorithm is decrypted. Return processing is continued to the management table searching step 1003.

[0035]When there is no data which is in agreement with the SQL sentence created at the search SQL sentence creation step 1002 in the management table 107, it progresses to the key table searching step 1005, the key table 108 is searched, and it is investigated whether there is still any line which is in agreement with the hash value calculated by the hash value calculation steps 1001. In the key table coincidence data check step 1006, the search results of the key table searching step 1005 are judged. When there is a line which is in agreement with the hash value calculated by the hash value calculation steps 1001, it returns to the search SQL sentence creation step 1002, and retrieval processing is performed using a new data encryption key. When there is no line which is in agreement with the hash value calculated by the hash value calculation steps 1001, it progresses to the search-results displaying step 1007. In the search-results displaying step 1007, search results are displayed on the screen of a client.

[0036]Next, processing of the search SQL sentence creation step 1002 is explained in detail using the flow chart of drawing 11. The search SQL sentence creation step 1002 consists of the encipherment information acquisition step 1100 and the encryption retrieved data creation step 1101. The key table 108 is searched with the encipherment information acquisition step 1100, and the data encryption key with which the line which is in agreement with the hash value calculated by the hash value calculation steps 1001 was enciphered, and the data encryption key which took out the encryption algorithm identifier and was enciphered are decoded with a key encryption key by it. In the encryption retrieved data creation step 1101, a search condition is enciphered as the decoded data encryption key by an encryption algorithm.

[0037]As a method of searching the database enciphered, it picks out one data at a time from the enciphered management table, The method and search condition which

investigate whether it is in agreement with a search condition are beforehand enciphered with the encryption key, decoding it, and there is a method of searching the management table enciphered by the enciphered search condition. In the former method, since processing of decoding occurs for every extraction of the data from a management table, the retrieval performance of a database is worsened greatly. Except that the processing which enciphers a search condition occurs once, the almost same retrieval performance as the database which is not enciphered can be taken out with the latter method. For this reason, the latter method is excellent in realization of search of the enciphered management table at the performance target. The latter method was explained in this example.

[0038]Since the keys used for encryption for every specific data set differed, the data encryption key was searched with the data structure of the method of this invention from the key table 108 using the hash value of data as a means which picks out the key which enciphers a search condition from the key table 108.

[0039]Drawing 12 shows the update process flow of the data to the encryption database which registration and the update control program 111 perform. A data update process, The update information input step 1200, the front [updating] data search step 1201, the coincidence data check step 1202, the serial number acquisition step 1203, the data-after-update encryption step 1204, the updating SQL sentence creation step 1205. And it consists of the database register step 1206. In the update information input step 1200, a user reads the data before updating inputted from the client 100, and the data after updating. The data before updating is searched with the data search step 1201 before updating from the management table 107. In the coincidence data check step 1202, the result searched with the data search step 1201 before updating is judged. An update process is ended when there is no data before updating searched with the data search step 1201 before updating in the management table 107.

[0040]When the data before updating searched with the data search step 1201 before updating is shown in the management table 107, it progresses to the serial number acquisition step 1203. In a serial number acquisition step, the serial number of the data before updating searched with the data search step 1201 before updating is acquired. In the data-after-update encryption step 1204, after calculating the hash value of the data after updating, the data after updating is enciphered with a data encryption key. A data encryption key is enciphered with a key encryption key. In the updating SQL sentence creation step 1205, the SQL sentence of the data to update is created using the data after the serial number acquired by the serial number

acquisition step 1203, and enciphered updating which were created at the data-after-update encryption step 1204. In the database register step 1206, the SQL sentence in which the updating execution program 124 created the data of the management table 107 at the update information SQL sentence creation step 1205 by the database management program 110 is performed and updated, The data encryption key enciphered as the hash value of the data after renewal of the key table 108 and an encryption algorithm identifier are updated.

[0041]Next, processing of the data search step 1201 before updating is explained in detail using the flow chart of drawing 13. The data search step 1201 before updating consists of the hash value calculation steps 1300, the encryption search condition creation step 1301, the management table searching step 1302, and the coincidence data check step 1303. In the hash value calculation steps 1300, the search condition preparing program 115 is started and the hash value of the data before updating is calculated. The enciphered data encryption key which starts the search condition preparing program 115, searches the key table 108 with the encryption search condition creation step 1301, and is in agreement with a hash value, and an encryption algorithm identifier are taken out. A data encryption key is decoded with a key encryption key, and a search condition is enciphered as the decoded data encryption key by the encryption algorithm 116. A retrieval execution program is started and the management table 107 is searched with the management table searching step 1302 by the SQL sentence enciphered at the encryption search condition creation step 1301. In the coincidence data check step 1303, it is investigated whether there is any data which is in agreement with the search condition of the SQL sentence created at the encryption search condition creation step 1301 to the management table 107. It ends, when there is data which is in agreement with the search condition of the SQL sentence created at the encryption search condition creation step 1301.

[0042]When there is no data which is in agreement with the search condition of the SQL sentence created at the encryption search condition creation step 1301, the another data encryption key and encryption algorithm identifier which are in agreement with a hash value and which were enciphered are taken out. The enciphered data encryption key is decoded with a key encryption key, a search condition is enciphered as the decoded data encryption key by the encryption algorithm corresponding to said encryption algorithm identifier, and the management table 107 is again searched with the enciphered search condition.

[0043]Next, processing of the data-after-update encryption step 1204 is explained in detail using the flow chart of drawing 14. The data-after-update encryption step 1204

consists of the hash value calculation steps 1400, the cryptographic algorithm determination step 1401, the data encryption step 1402, and the key encryption step 1403. The hash value of the data after updating is calculated in the hash value calculation steps 1400. In the cryptographic algorithm determination step 1401, the enciphered program 120 determines the encryption algorithm used for this encryption. The enciphered program 120 can have two or more cryptographic algorithms, and he is trying to use in it the cryptographic algorithm most newly registered into the enciphered program 120 for encryption at the time of registration and updating. In the data code step 1402, a data encryption key is created and the data registered into the management table 107 is enciphered. In the key encryption step 1403, a data encryption key is enciphered with the key encryption key in the key storage area 128.

[0044]Drawing 15 shows the deletion flow of the data of the encryption database which the deletion control program 113 performs. Data deletion consists of the supersession data input step 1500, the supersession data searching step 1501, the coincidence data check step 1502, the serial number acquisition step 1503, the deletion SQL sentence creation step 1504, and the database deletion execution step 1505. In the supersession data input step 1500, a user reads the data which was inputted from the client 100 and to delete. Supersession data is searched with the supersession data searching step 1501. In the coincidence data check step 1502, it is confirmed whether the supersession data searched with the supersession data searching step 1501 is shown in the management table 107. Deletion is ended when there is no supersession data searched with the supersession data searching step 1501 in the management table 107.

[0045]When the supersession data searched with the supersession data searching step 1501 is shown in the management table 107, it progresses to the serial number acquisition step 1503. In the serial number acquisition step 1503, the serial number of the supersession data searched with the supersession data searching step 1501 is acquired. In the deletion SQL sentence creation step 1504, a deletion SQL sentence is created using the serial number acquired by the serial number acquisition step 1503. In the database deletion execution step 1505, the line of the serial number acquired from the management table 107 and the key table 108 by the serial number acquisition step 1503 using the deletion SQL sentence created at the deletion SQL sentence creation step 1504 is deleted. It returns to the supersession data searching step 1501, and processing is continued.

[0046]As mentioned above, a set of a value with a management table and its table specific as a feature of this example (Field) the information (an encryption key and an

encryption algorithm identifier.) for the encryption about a line, a sequence, etc. The database structure managing confidential information with a key table with the hash value of data and the registration processing of the data in the composition, retrieval processing, an update process, and deletion were explained. According to this example, the safety of the enciphered database can be improved by changing an encryption key dynamically at the time of data registration or updating, and another managing the information for encryption with a management table using said database structure. It is also possible to become possible to use different encryption algorithms for every set of the specific value of a management table, and to perform the change of an encryption key and an encryption algorithm dynamically during database operation further. Therefore, by applying this example, the safety of enough databases is securable.

[0047]Next, the second example of this invention is described. Although this example takes the same composition as the first example shown in drawing 1, the portion which updated the data encryption key also at the time of search differs from the first example. The retrieval system of the second example is explained using drawing 16. Data retrieval processing of the second example, The retrieved data input step 1600, the hash value calculation steps 1601, the search SQL sentence creation step 1602, the management table searching step 1603, the management table coincidence data check step 1604, the key table searching step 1605, It consists of the key table coincidence data check step 1606, the search-results displaying step 1607, the serial number acquisition step 1608, all the data decryption steps 1609, the key table recording step 1610, and the management table recording step 1611.

[0048]The processing from the retrieved data input step 1600 of drawing 16 to all the data decryption steps 1609 is equivalent to processing from the retrieved data input step 1000 of drawing 10 to all the data decryption steps 1009, respectively, and performs the same processing. In the key table recording step 1610, the data encryption key for enciphering the data which was in agreement with the search condition is newly created, the data encryption key is enciphered with a key encryption key, and it registers with the key table 108 with a serial number and an encryption algorithm identifier. In the management table recording step 1611, after enciphering the data which was in agreement with the search condition using the data encryption key created by the key table recording step 1610 and registering with the management table 107, it returns to the management table searching step 1603, and search of the management table 107 is continued.

[0049]In the above, the method which changes an encryption key not only at the time

of data registration or updating but at the time of search was explained as the second example. According to this example, the safety of the database enciphered in order to update an encryption key more frequently than the time of the data registration of the first example or updating can be further improved using said database structure by changing an encryption key dynamically at the time of data registration, updating, or search.

[0050]Next, the third example of this invention is described. In the first example, when a new encryption algorithm was added, it was used promptly. Although this example takes the same composition as the first example shown in drawing 1, the portion which specifies an encryption algorithm in a higher rank and enciphered it by the specified encryption algorithm differs from the first example.

[0051]This example is described using drawing 1. The outline of the registration processing of the data enciphered and stored in a database is explained. A user inputs the data registered into a database from the client 100, and specifies an encryption algorithm identifier. Registration and the update control program 111 are started, and the encryption algorithm identifier specified as the data which was inputted from the client 100, and to register is passed to registration and the update control program 111. Registration and the update control program 111 pass the data and the encryption algorithm identifier which are registered into registration / updating preparation program 117. Registration / updating preparation program 117 creates a serial number by the initial condition preparing program 118, Calculate hash of the data registered by the hash value calculation program 119, and the data encryption key based on the encryption algorithm identifier specified by the enciphered program 120 by the client 100 is created, The data registered using this key is enciphered and it enciphers with the key encryption key which is in the key storage area 128 by the encryption algorithm in which the key enciphered program 121 has that data encryption key further.

[0052]Registration / updating preparation program 117 passes the encryption algorithm identifier which enciphered a serial number, the hash value of the data registered, the enciphered registration data, a data encryption key, and registration data to registration and the update control program 111. Registration and the update control program 111 pass these data to registration and the renewal condition preparing program 122. Registration and the renewal condition preparing program 122 create the SQL sentence for the management table 107 and the key table 108 from the passed data, respectively, and passes it to registration and the update control program 111. Registration and the update control program 111 pass the SQL sentence

created by registration and the renewal condition preparing program 122 to the registration execution program 123. The registration execution program 123 using the database management program 110 to the management table 107. A serial number and the enciphered registration data are registered and the encryption algorithm identifier which enciphered a serial number, the hash value of the data registered, a data encryption key, and registration data to the key table 108 is registered.

[0053]Next, the outline of the update process of data in the third example is explained. A user specifies the encryption algorithm identifier of the data before updating, the data after updating, and the data after updating from the client 100. Registration and the update control program 111 are started, and the parameter inputted from the client 100 is passed to registration and the update control program 111. Registration and the update control program 111 pass the data before updating to the data search program 114. The data search plug rum 114 enciphers the data before updating by the search condition preparing program 115, takes out the serial number of the data before updating by a retrieval execution program, and passes it to registration and the update control program 111. Registration and the update control program 111 pass the encryption algorithm identifier which enciphers a serial number, the data after updating, and the data after updating to registration / updating preparation program 117.

[0054]Registration / updating preparation program 117 by a hash value calculation program. Calculate the hash value of the data after updating and the data encryption key based on the encryption algorithm which enciphers the data after updating specified by the enciphered program 120 by the client 100 is created, The data to update is enciphered and the key enciphered program 121 enciphers the data encryption key further by the encryption algorithm which the key enciphered program 121 has with the key in the key storage area 128. Registration / updating preparation program 117 passes the hash value of the data after updating, the enciphered data, the enciphered data encryption key, and an encryption algorithm identifier to registration and the update control program 111. Registration and the update control program 111 pass a serial number, the hash value of the data after updating, the enciphered data, the enciphered data encryption key, and an encryption algorithm identifier to registration and the renewal condition preparing program 122. Registration and the renewal condition preparing program 122 create the SQL sentence for the management table 107 and the key table 108 from the passed data, respectively, and passes it to registration and the update control program 111. Registration and the update control program 111 pass the SQL sentence created by registration and the

renewal condition preparing program 122 to the updating execution program 124. The updating execution program 124 updates the hash value of the data of the management table 107, and the data of the key table 108, the enciphered data encryption key, and an encryption algorithm identifier using the database management program 110.

[0055]As explained above, according to the third example, high order application can specify an encryption algorithm freely, and can choose an encryption algorithm flexibly.

[0056]As mentioned above, a data set with a management table and its table specific as a feature of this invention (Field) the information (an encryption key and an encryption algorithm identifier.) for the encryption about a line, a sequence, etc. The database structure managing confidential information with a key table with the hash value of data, Registration of the enciphered data in the composition, search, updating, deletion, the dynamic updating method of an encryption key, and how to change the encryption algorithm under database operation were explained. As a database management system which this invention uses, either a relational database or an object oriented database is feasible.

[0057]An object will be used for the definition of the key table 108 when using an object oriented database. The field of a hash algorithm can be added to the key table 108, and a hash algorithm can also be changed into it for every specific data set with an encryption algorithm.

[0058]According to this invention, the safety of the enciphered database can be improved by changing an encryption key dynamically and another managing the information for encryption with a management table using said database structure. It is also possible to become possible to change into a new encryption algorithm for every specific data set, and to perform the change of an encryption key and an encryption algorithm dynamically during database operation. Therefore, by applying this invention, the safety of enough databases is securable. Also when an encryption algorithm still firmer than the future is invented, the algorithm for management data codes can be changed to a dynamic more firm method.

[0059]

[Effect of the Invention]According to this invention, in the enciphered database, the change of an encryption key and an encryption algorithm can be dynamically performed during database operation, and a safe confidential information management data base with pliability can be created.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the composition of one gestalt of operation of the confidential information managing system of the database of this invention.

[Drawing 2]It is a figure for explaining the management table of the database enciphered for every field.

[Drawing 3]It is a figure for explaining the key table of the database enciphered for every field.

[Drawing 4]It is a figure for explaining the management table of the database enciphered for every line.

[Drawing 5]It is a figure for explaining the key table of the database enciphered for every line.

[Drawing 6]It is a figure for explaining the management table of the database enciphered for every sequence.

[Drawing 7]It is a figure for explaining the key table of the database enciphered for every sequence.

[Drawing 8]It is a flow chart explaining the procedure of the data registration of a database performed by this invention.

[Drawing 9]It is a flow chart explaining the procedure of registration / updating preparation program at the time of the data registration of a database performed by this invention.

[Drawing 10]It is a flow chart explaining the procedure of the data retrieval of a database performed by this invention.

[Drawing 11]It is a flow chart explaining the procedure of the search condition preparing program at the time of the data retrieval of a database performed by this invention.

[Drawing 12]It is a flow chart explaining the procedure of the renewal of data of a database performed by this invention.

[Drawing 13]It is a flow chart explaining the procedure of the data search program at the time of the renewal of data of a database performed by this invention.

[Drawing 14]It is a flow chart explaining the procedure of registration / updating

preparation program at the time of the renewal of data of a database performed by this invention.

[Drawing 15]It is a flow chart explaining the procedure of the data deletion of a database performed by this invention.

[Drawing 16]It is a flow chart explaining the procedure of the data retrieval accompanied by the encryption key of a database and change of an encryption algorithm which are made by this invention.

[Description of Notations]

100 Client
101 LAN
102 LAN adapter
103 Server
104 CPU
105 Bus
106 Magnetic disk drive
107 Management table
108 Key table
109 Main memory
110 Database management program
111 Registration and an update control program
112 Search control program
113 Deletion control program
114 Data search program
115 Search condition preparing program
116 Retrieval execution program
117 Registration / updating preparation program
118 Initial condition preparing program
119 Hash value calculation program
120 Enciphered program
121 Key enciphered program
122 Registration and a renewal condition preparing program
123 Registration execution program
124 Updating execution program
125 Key acquisition program
126 Deletion-conditions preparing program
127 Deletion execution program

128 Key storage area

[Translation done.]